NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

EXPLOITATION OF EXISTING VOICE OVER INTERNET PROTOCOL TECHNOLOGY FOR DEPARTMENT OF THE NAVY APPLICATION

By

Henry M. Vegter Jr.
David T. Wallace

September 2002

Thesis Advisor: Dan Boger
Second Reader: Rex Buddenberg

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2002	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE: Title (Mix case letters) Exploitation of Existing Voice over Internet Protocol Technology for Department of the Navy Application	**5. FUNDING NUMBERS**
6. AUTHOR(S) **David T. Wallace, Capt, USMC and Henry M. Vegter Jr., LT, USN**	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Space and Naval Warfare Systems Command, San Diego, CA	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT *(maximum 200 words)*

This thesis documents an investigation into the technology of Voice over Internet Protocol (VoIP). VoIP promises to be a widely accepted technology in the future. The issues of efficient use of bandwidth over network choke points, cost savings gained from a common data and voice infrastructure, reduced cost associated with toll calls and the merger of the telephone with the desktop will keep adoption of this technology on the path to ubiquitous use.

Topics explored in the thesis include convergence over IP infrastructure, the status of VoIP technology available and providers in the VoIP industry. A prototypical cost benefit analysis of implementing VoIP is presented using NPS as an example.

Convergence on bandwidth restricted satellite links offers the most promising application of VoIP in the DoN today. A test network is constructed demonstrating the feasibility of implementing VoIP on the Automated Digital Network System (ADNS). Quality of Service (QoS) features enable further enhancements in throughput.

14. SUBJECT TERMS Voice over Internet Protocol, VoIP, Convergence, ADNS, Cost Benefit Analysis, Quality of Service, QoS	**15. NUMBER OF PAGES** 127
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

EXPLOITATION OF EXISTING VOICE OVER INTERNET PROTOCOL TECHNOLOGY FOR DEPARTMENT OF THE NAVY APPLICATION

David T. Wallace
Captain, United States Marine Corps
B.S., University of Illinois, 1995

Henry M. Vegter Jr
Lieutenant, United States Navy
B.S., Eastern Michigan University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2002

Author: David T. Wallace

Author: Henry M. Vegter Jr

Approved by: Dan C. Boger
Thesis Advisor

Rex A. Buddenberg
Second Reader

Dan C. Boger
Chairman, Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis documents an investigation into the technology of Voice over Internet Protocol (VoIP). VoIP promises to be a widely accepted technology in the future. The issues of efficient use of bandwidth over network choke points, cost savings gained from a common data and voice infrastructure, reduced cost associated with toll calls and the merger of the telephone with the desktop will keep adoption of this technology on the path to ubiquitous use.

Topics explored in the thesis include convergence over IP infrastructure, the status of VoIP technology available and providers in the VoIP industry. A prototypical cost benefit analysis of implementing VoIP is presented using NPS as an example.

Convergence on bandwidth restricted satellite links offers the most promising application of VoIP in the DoN today. A test network is constructed demonstrating the feasibility of implementing VoIP on the Automated Digital Network System (ADNS). Quality of Service (QoS) features enable further enhancements in throughput.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

ACAT	Acquisition Category
ACELP	Algebraic Code Excited Linear Prediction
ACF	Admission Control Message
ADNS	Automated Digital Network System
AFCEA	Armed Forces Communications and Electronics Association
ALI	Automatic Location Identification
ANI	Automatic Number Identification
ARG	Amphibious Ready Group
ARJ	Admission Reject Message
ARQ	Admission Request Message
ASCII	American Standards Code for Information Interchange
ATM	Asynchronous Transfer Mode
AVVID	Architecture for Voice, Video, and Integrated Data
BG	Battle Group
CA	Certificate Authority
CAG	Call Agent
CC	Country Code
CELP	Code Excited Linear Prediction
CIO	Chief Information Officer
CLAN	Control Local Area Network
CLI	Command Line Interface
CM	Call Manager
CNO	Chief of Naval Operations
CODEC	Compression Decompression
COMOPTEVFOR	Commander, Operational Test and Evaluation Force
COMTHIRDFLT	Commander, Third Fleet
CoS	Class of Service
CVBG	Carrier Battle Group
DCE	Digital Communications Equipment
DHCP	Dynamic Host Control Protocol
DiffServ	Differential Services
DNS	Domain Name Server
DoN	Department of the Navy
DTE	Digital Terminal Equipment
DTMF	Dual Tone Multi Frequency
E9-1-1	Enhanced 911 Emergency Services

ECLIPS	Enterprise Class IP Soutions
E-commerce	Electronic Commerce
EHF	Extra High Frequency
ESE	Enterprise Solution Engineering
FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber
HF	High Frequency
HTTP	Hypertext Protocol
ICT	Inter-Cluster Trunk
IDIQ	Indefinite Delivery, Indefinite Quantity
IETF	Internet Engineering Task Force
InterNIC	Internet Network Information Center
IP	Internet Protocol
IPSec	Internet Protocol Security Tunnel Mode
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU-T	International Telecommunications Union – Telecommunications Standards Committee
KG	Key Generator
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LLQ	Low Latency Queuing
MAC	Media Access Control
MarCorSysCom	Marine Corps Systems Command
MARFORPAC	Marine Forces Pacific
MEGACO	Media Gateway Control
MGCP	Media Gateway Control Protocol
MLPP	Multi-Level Precedence and Preemption
MoIP	Multi-Level Precedence and Preemption over Internet Protocol
MOS	Mean Opinion Score
MP-MLQ	Multi-Pulse -- Maximum Likelihood Quantizer
MTBF	Mean Time Between Failure
NAVSEA	Naval Sea Systems Command
NCTAMS	Navy Computer and Telecommunications Area Master Station
NDC	National Destination Code
NES	Network Encryption System
NMCI	Navy Marine Corps Intranet

NOC	Network Operations Center
NPS	Naval Postgraduate School
NPV	Net Present Value
NSA	National Security Administration
NSN	National Significant Number
PBX	Public Branch Exchange
PC	Personal Computer
PCM	Pulse Code Modulation
PKI	Public Key Infrastructure
POP	Point of Presence
POTS	Plain Old Telephone Service
PPTP	Point-to-Point Tunneling Protocol
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
QoS	Quality of Service
R Factor	Rating Factor
R&D	Research and Development
RA	Registration Authority
RAS	Registration/Admission/Status
RF	Radio Frequency
RFC	Requests for Comment
RTCP	Real-time Control Protocol
RTP	Real-time Transport Protocol
SBBL	Sea-Based Battle Lab
SCCP	Skinny Client Control Protocol
SCORE	Southern California Offshore Range
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SPAWAR	Space and Naval Warfare Systems Center
SS7	Signaling System 7
SSh	Secure Shell
STU-III	Secure Telephone Unit, Generation III
SUBPAC	Submarine Force, U.S. Pacific Fleet
SURFLANT	Naval Surface Force, U.S. Atlantic Fleet
TACLANE	Tactical FASTLANE KG-175
TCP	Transmission Control Protocol

TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UMS	Unified Messaging Server
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VWIC	Voice Wire Interface Card
WRR	Weighted Round Robin
XML	Extensible Markup Language

ACKNOWLEDGMENTS

Without the help of the following people this thesis would not have been possible:

From Cisco Systems

Dave West

Peter Labbe

Charlie Booth

From SPAWAR San Diego CA

Eric Otte

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Voice over Internet Protocol (VoIP) promises to be a widely accepted technology in the future. The issues of efficient use of bandwidth over choke points, cost savings gained from a common data and voice infrastructure, reduced cost associated with toll calls and the merger of the phone with the desktop will keep adoption of this technology on the path to ubiquitous use.

Protocols for VoIP are still developing and industry standards have not yet been reached. These two facts create obstacles to implementing a VoIP solution today. Current limiting factors are incompatibility between vendors, no support for MLPP, and the lack of a NSA approved secure VoIP terminal. An enterprise VoIP solution adopted today would need to be supplied by a single industry leader.

Convergence should be a long-term goal as it promises the most efficient use of network resources. The economic advantages of convergence should be evaluated for each implementation. This thesis presents an example of a cost benefit analysis of installing VoIP.

Convergence on bandwidth restricted satellite links offers the most promising application of VoIP in the DoN today. A network configuration demonstrating one possible implementation of VoIP over ADNS was constructed. Connectivity tests, operational tests, and bandwidth stress tests were conducted on this network. The utility of QoS and convergence was demonstrated by flooding the network with traffic both before and after QoS features were enabled. Utilizing QoS features resulted in a 26 percent increase in allowable TCP traffic over the converged simulated satellite link.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND TECHNICAL REVIEW

A. ISSUES LEADING TO VOIP

Voice over Internet Protocol, or VoIP, is an emerging technology that offers more efficient ways to do things that can already be done, such as convey voice conversation, as well as new capabilities that are only possible through combining voice and data networks. Combining voice and data network infrastructure is commonly referred to as convergence. The efficiencies gained through convergence offer the most compelling reasons for advancing VoIP technology.

Despite the fact that VoIP is only recently emerging at the desktop, traditional phone service providers have long used the underlying technology. The days of circuit switched telephony from end to end are passed. In the modern Public Switched Telephone Network (PSTN), circuit-switched networks only exist between the end user and the local switch. Thereafter, voice messages are broken down into packets and sent over connectionless networks to the switch at the receiving end. The advent and rapid growth of the Internet extends this capability to the desktop. While the phone companies have long realized the advantages of packetized voice, these advantages are only now emerging in the Internet age at the desktop. Table 1 lists some of the advantages offered by VoIP.

Advantages of VoIP
1. More efficient use of available bandwidth provides economy of scale 2. Cost savings in common infrastructure 3. Cost savings on toll calls 4. New applications made possible

Table 1. Advantages of VoIP (After Ref. [1])

1. Bandwidth Usage

When a traditional circuit-switched call is set up, the entire bandwidth dedicated to the call is reserved for the duration of the call. In a typical conversation, 36-40 percent of the conversation is silence. Thus nearly half of the bandwidth is wasted transmitting no information. Through a method known as silence suppression, packetized voice offers the advantage of allowing the receiving end to generate its own silence without burdening the network, thereby freeing bandwidth for other IP traffic.

DoN networks are configured with a specified amount of bandwidth reserved for voice conversations. By eliminating these reserved channels, VoIP allows the bandwidth reserved for voice conversations to be dynamically assigned to other IP traffic. Artificial bandwidth constraints are eliminated and the limited bandwidth available is more efficiently allocated on an as-needed basis.

2. Common Infrastructure

DoN installations currently have both a Plain Old Telephone Service (POTS) infrastructure and a data network infrastructure. Significant funds are spent upgrading and replacing Public Branch Exchanges (PBX) and telephones. VoIP promises to eliminate these redundant expenses. Dynamic allocation of bandwidth usage on a common IP infrastructure ultimately leads to more efficient use of available bandwidth. Efficiencies of common infrastructure are especially critical in the bandwidth choke point of ship to shore communication links.

The largest portion of network life cycle cost is attributed to the salary of the personnel operating and maintaining the network. Obviously the management of a single network provides significant financial savings over managing two networks. The management burden of a converged network increases beyond what it was for either of stand-alone networks.

Through the use of vendor-supplied software such as Chariot VoIP Assessor from NetIQ Corporation[1], networks can be tested for suitability of carrying VoIP traffic. Initial testing can reveal bottlenecks in the network that pose potential problems for VoIP. Even if VoIP is not the immediate solution, armed with the analysis results supplied by assessor software, administrators can make future upgrades to network infrastructure tailored to accommodate VoIP support. Convergence in existing installations can be viewed as a long-term savings. New installations, on the other hand,

[1] NetIQ is one of many vendors selling network analysis tools. Their website for Chariot VoIP Assessor can be found at http://www.netiq.com/products/va/default.asp

can start with a single IP infrastructure and avoid legacy circuit-switched infrastructure expense.

3. Toll Fee Savings

Using the Internet to route voice traffic between distant ends eliminates the PSTN infrastructure previously required to carry the conversation. The cost of accessing the PSTN is thereby eliminated. In cases where Internet connectivity does not reach the distant end, VoIP allows a caller to initiate the PSTN call from a local switch to the destination. Once again, toll fees are avoided or reduced.

4. New Capabilities

Since VoIP and networked data are both encapsulated in IP datagrams, future applications can merge the two. Applications that incorporate voice recognition and voice mail translation to text are two examples of new capabilities enabled by VoIP.

B. BACKGROUND OF VOIP TECHNOLOGY

VoIP is the conversion of analog digital communications into digital packets of data transmitted over an Internet Protocol (IP) based network. An IP network carries multiple voice conversations in the same bandwidth as one PSTN phone call. For example a single uncompressed PSTN phone call theoretically requires 64-kbps and a VoIP call requires 18-kbps (with G.723.1 MP-MLQ compression), including protocol overhead. VoIP is digitized voice signal sliced into packets and sent with other IP packets across a packet switched network. At the receiving end, the packets are reassembled and arrive as a normal sounding voice telephone call. VoIP is an emerging technology that currently allows Phone-to-Phone, PC-to-PC, PC-to-Phone, Phone-to-PC and fax-to-fax services, all over an IP network. To understand the significance of this emerging technology a reference of current technology is needed.

1. Traditional Phone System

The technology used in modern telephones dates back to the turn of the 20th century, when the only way to make a phone call was to ring an operator and have a call physically patched to the desired destination. Out of this labor-intensive process many improvements and modifications were made to reduce labor and cost per use. Currently the providers of the PSTN phone system are looking for innovative ways to continue the process of cost reduction and still provide the quality of service (QoS) and availability users of the telephone in North America have come to expect. The availability that is expected from PSTN is 99.999%. This means the network can be down less than 6 minutes of the 525,600 minutes each year. The PSTN telephone service provided today is given the acronym of POTS (plain old telephone service). When an individual desires to make a call, the caller picks up the handset and hears an audible tone (dial tone). When a number is dialed, it specifies the address of the phone to be called. The PSTN utilizes Signaling System 7 (SS7) to set up a circuit for the call, reserving capacity and bandwidth over the backbone. Calls destined outside the local access are routed though a Point of Presence (POP). The destination phone rings, indicating an incoming call. When the receiving handset is picked up the conversation takes place. When a path is selected it is maintained for the entire length of the call. A system level depiction of a legacy phone system is shown in Figure 1. After the phone call is terminated, the circuit is broken down and the resources are released for allocation.

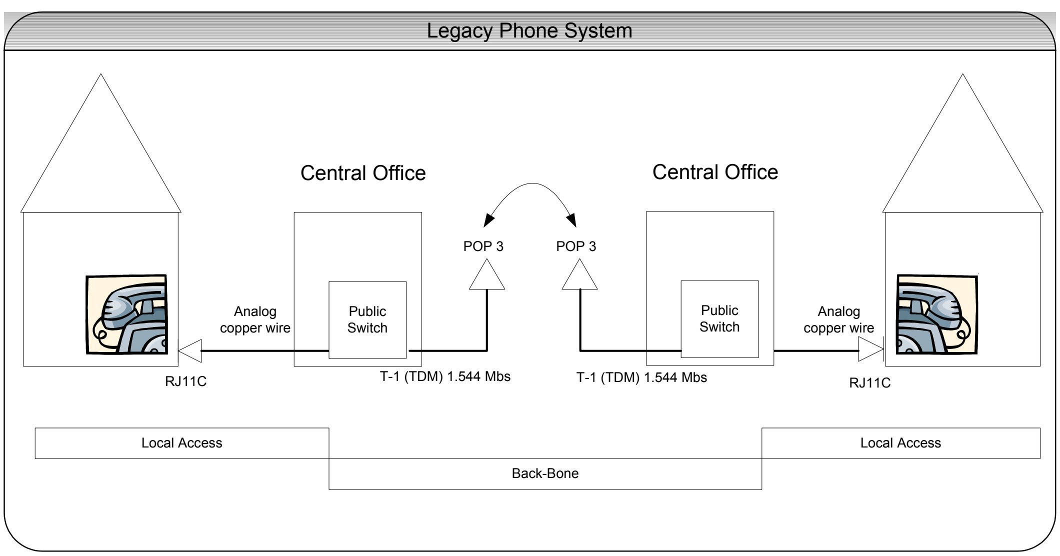

Figure 1. Legacy Phone System (After Ref. [2])

The Mean Opinion Score (MOS) is used to indicate PSTN phone call quality. The MOS is defined by the International Telecommunication Union - Telecommunications Standards Committee (ITU-T).[2] The MOS provides a subjective measurement of voice quality based on a numeric score ranging from one to five, with 1.0 representing Not Recommended and 5.0 representing Very Satisfied. PSTN technology utilizes the ITU-T Recommendation E.164, International Public Telephone Numbering Plan, for addressing and Dual Tone Multi Frequency (DTMF) for signaling. The E.164 numbering plan provides a maximum of 15 digits in three different networks. The three networks are National, Global, and International telephone networks. All three networks utilize a country code (CC) and a National Significant Number (NSN). The NSN is divided into two segments, the National Destination Code (NDC) and a Subscriber Number (SN).[3] To relay addressing in analog form between a phone and public switch, DTMF is used. Sometimes referred to as "touch tone," a DTMF signal consists of the sum of two pure sinusoids at valid frequencies as shown in Figure 2. When a number is selected the sum of the two frequencies provide the resulting tone to the public switch. The public switch interprets the tones as the address of the desired call.

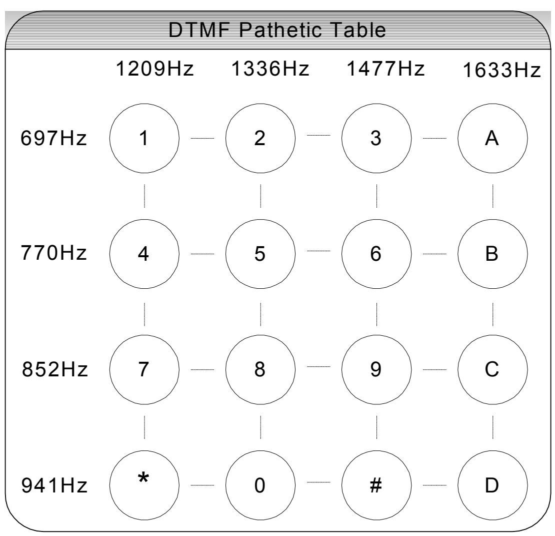

Figure 2. DTMF Pathetic Table (After Ref. [3])

[2] The ITU is a United Nations organization created for governments and private sector to coordinate global networks and telecommunications systems. The Telecommunications Standards Committee is one of three sectors of the ITU and is responsible for telecommunications standards.

[3] For additional information on telephone numbering plans visit http://www.itu.int/itudoc/itu-t/ob-lists/icc/e164_717.html, (March 2002)

2. VoIP Comparison

What makes a VoIP call different than a PSTN phone call? To an end user the VoIP call provides the same service as a PSTN call. The major difference comes from the way the call is connected, bandwidth used and the capacity that is reserved. During VoIP call setup, dial tone, DTMF, ringing, and busy signals are emulated by the terminal or the gatekeeper. The audio portion of the call is converted from analog to digital, divided up into packets, encapsulated in IP data grams and sent across a network. At the receiving switch the packets are stripped of the IP encapsulation, assembled and converted from digital to analog form. A simple diagram of this digitization process is shown in Figure 3.

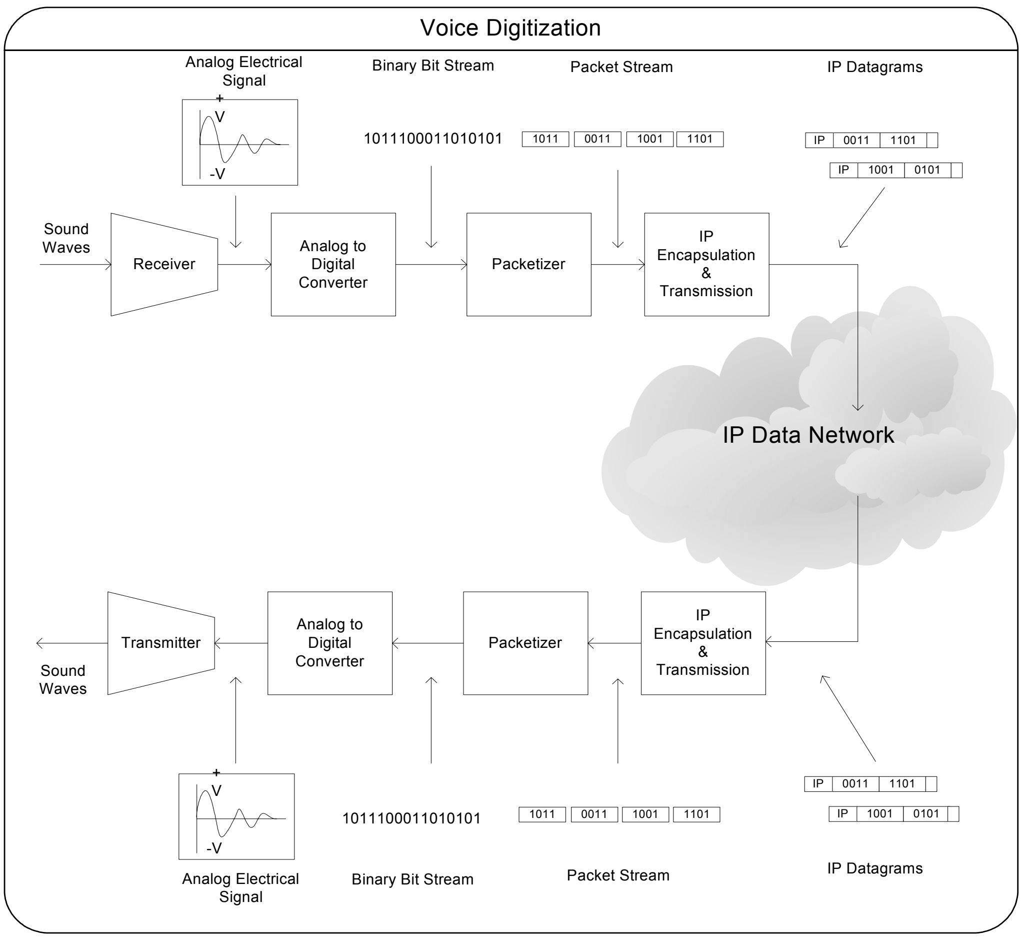

Figure 3. Simple Diagram of VoIP Transport Process (After Ref. [4])

When an individual desires to make a call, the caller picks up the handset and hears audible tone (dial tone). When a number is dialed, it specifies the address of the phone to be called, which is mapped to an IP address. Call setup protocols are used to locate the recipient and send a signal to produce a ring. Generally, TCP is used for call setup, serving the same function as SS7 does in the POTS backbone. The destination phone rings, indicating an incoming call. When the receiving handset is picked up the conversation takes place. UDP is used for the real-time transmission of encoded voice IP data grams. The audio information is encoded and travels over the IP network using one of the voice streaming protocols.

The current dominant Internet Protocol addressing scheme is IPv4 (Version 4). An IPv4 consists of a 32-bit number, which allows for more than 4.2 billion IP addresses. There is one central authority for allocating IP addressees for networks connected to the worldwide Internet; that authority is the InterNIC (Internet Network Information Center). IPv6 (Version 6) is completed and in limited use. The motivating factor for migration to IPv6 is the number of addresses available to build a network. IPv6 provides over 340 x 10^{36} IP addresses.

C. COMPONENTS OF VOIP

A VoIP network consists of three primary components – terminals, gateways, and gatekeepers. A terminal or endpoint can be a soft phone on a PC, an IP desk phone, or a traditional analog phone connected through a gateway.

1. Gateway

A gateway is a node on a LAN that communicates with other LAN components and translates between network and signaling formats. The gateway provides for real-time, two-way communications between terminals on the network. The gateway receives packetized voice transmissions from users within the network and then routes them to other parts of the network using a specified medium (T-carrier, E-carrier or Satellite interface). The IP address of the destination gateway is then used to route the telephone call as packets through the IP network. This process is reversed to provide a full duplex conversation. The gateway is responsible for emulating call signals of the traditional phone system.

2. Gatekeeper

The Gatekeeper is also known as a Call Agent (CAG), it serves as the primary control agent of Internet telephony networks. The Gatekeeper is the address resolution component; it matches dialed phone numbers to IP addresses. A gatekeeper is the entity on the network that provides the management capabilities for commercial VoIP. Gatekeeper functionality includes the following:

- Authentication and authorization of users
- Authentication and authorization of network elements, such as telephony gateways
- Call routing, determined by factors such as quality of service (QoS), Communications media capabilities, and user ID
- Least cost routing
- Load balancing
- Account and call capabilities
- Address resolution
- Call forwarding to a variety of endpoint devices like pagers, fax machines and PCs

D. VOIP PROTOCOLS

The protocols utilized by VoIP are transforming. Currently several protocols are struggling to become the VoIP standard. H.323 and SIP are the front-runners. H.323 has become the unofficial industry standard for most producers of VoIP infrastructures.

1. H.323 Standard

H.323 is an ITU-T standard that was created in 1996 and updated in 1998 and again in 2000. It provides a foundation for audio, video and data communications across packet-based network infrastructure. H.323 is not just one protocol. It is really a suite of protocols that interact to provide packet-based multimedia communications. H.323 provides standards for encoding, simple bandwidth management, admission control, address translation, call control and management, and links to external networks. H.323 Version 2 was developed with emphasis on voice, rather than multimedia capability of Version 1. H.323 Version 3 is developed, but not yet widely implemented and is designed to support large-scale commercial production networks [Ref 1].

The H.323 protocol stack consists of a set of protocols that ride on top of TCP/IP and UDP/IP (Figure 4). TCP is used for call set up and control. UDP is utilized for data transmission and reception. Interoperability is provided by H.245, which provides a standard method of call connection and capabilities negotiation using modified Q.931 signaling. H.245 makes use of TCP as a transport for this control data. H.245 signaling is established between two endpoints, or an endpoint and a gateway. The endpoint establishes one H.245 control channel for each call.

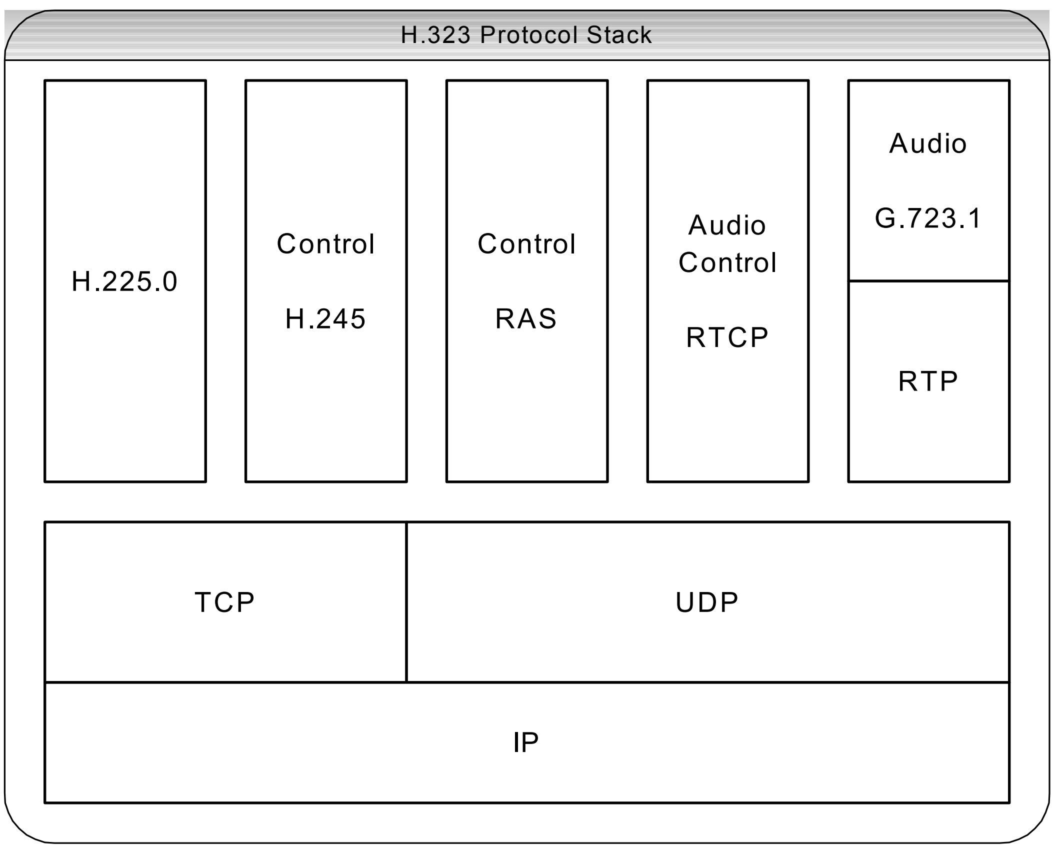

Figure 4. H.323 Protocol Stack (After Ref. [5])

H.225.0 is the data transport standard. H.225.0 communicates with Real-time Transport Protocol (RTP) to identify the payload type and time-stamp data, and communicates with the Real-time Transport Control Protocol (RTCP) to determine control information. The RTP and RTCP data is delivered by H.225.0, which guarantees delivery with TCP.

Q.931 is used with RAS (Registration/Admission/Status) to support call initiation as shown in Figure 5. RAS Messages (Setup, Call Proceeding and Alerting) are used between the endpoints and Q.931 messages, ARQ (Admission Request Message), ACF (Admission Confirmation Message), and ARJ (Admission Reject Message) are exchanged between H.323 terminals.

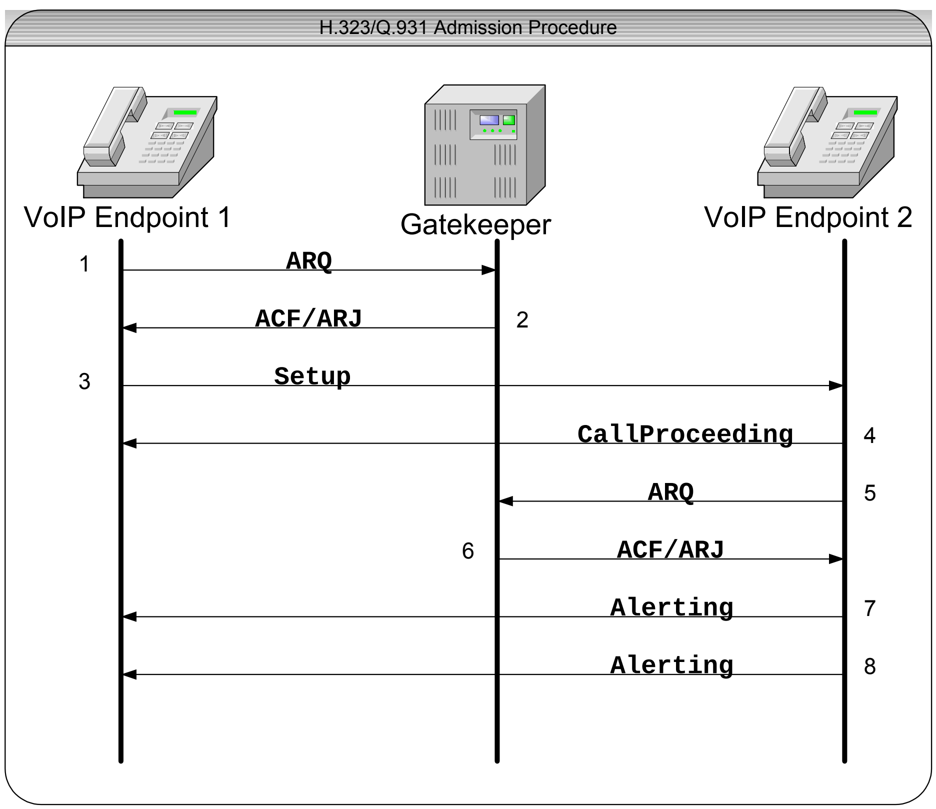

Figure 5. H.323/Q.931 Admission Procedure (After Ref. [1])

Elachi, points out that the time and complexity involved in setting up a call is the complaint most often raised about H.323. The protocol uses multiple roundtrip messages to establish signaling and control for any call between two terminals. Additionally, H.323 requires that TCP connections be used to carry the control messages. Each TCP connection involves a three-way exchange for set-up and an additional transmission for acknowledgement of receipt. The recently released version 3 is an improvement and includes a "Fast Connect" procedure that effectively consolidates the Q.931 messages exchanged between terminals and implements a tunneling procedure that lets H.245 share a single TCP connection with Q.931. Since each TCP connection setup consists of a three-way handshake, doing the entire setup with a single TCP connection reduces overhead. [Ref. 7]

2. Real-Time Transport Protocol

As the name suggests, Real-time Transport Protocol or RTP provides real-time delivery of data. Various protocols can be used to set up, modify and tear down VoIP sessions but RTP is required to carry the actual voice traffic. Internet Engineering Task Force (IETF)[4] RFC 1889 and RFC 1890 cover the minimum requirements for interoperability of RTP. Since real-time applications cannot wait for acknowledged receipt from the distant end, RTP is typically built on UDP, though other transport protocols can carry RTP traffic. UDP provides RTP the ability to error check and multiplex. Figure 4 shows how RTP relates to the UDP/IP stack. The connectionless, best-effort delivery inherent in UDP is inadequate for reconstructing real-time voice and video signals so RTP includes a sequencing system to detect missing packets. RTP also includes information regarding the payload type including the audio and video encoding used in the RTP packet, whether or not silence suppression is used and source identification.

To monitor network and application performance a control protocol called Real-time Transport Control Protocol, RTCP, is used. RTCP is not required for RTP to work and, consequently, the IETF recommends that RTCP traffic be limited to five percent of the total RTP traffic. Periodically, session participants send an RTCP/UDP/IP packet indicating reception and transmission statistics. The information contained in the RTCP

[4] The IETF is an organization open to parties from the international community who are interested in the evolution of the Internet architecture and the smooth operation of the Internet. The IETF publishes their recommendations in the form of Requests for Comment (RFC). RFC's are generally accepted as standards definitions. Their website can be found at http://www.ietf.org, (March 2002)

packet can be used to adjust transmissions, determine where problems are occurring, and evaluate network performance.

RTP packets are the greatest contributors to VoIP network traffic. Since they utilize UDP/IP transport they also pose specific network problems, especially when they are routed through firewalls. Many firewalls are not configured to allow UDP traffic to pass. Currently, firewalls operated by the Navy Fleet Network Operations Center (NOC), the agency responsible for controlling network traffic within the DoN, block certain UDP ports. Various methods of overcoming the firewall obstacle are being explored commercially. Proprietary routers and software that scan incoming UDP packets and allow RTP traffic to pass introduce network delays that may not be acceptable. Address translation in firewalls further exacerbates the situation by modifying addresses in data streams. The easiest but least secure method of preventing firewall interference is to place the VoIP gateway outside the firewall.

3. Session Initiation Protocol

H.323 is considered by many to be too complex and difficult to code, resulting in expensive gateways; its peer-to peer architecture also makes it difficult to scale. Session Initiation Protocol or SIP, described in RFC 2543, is the IETF replacement for H.323. SIP, like HTTP and SMTP, is a text based signaling protocol sent over TCP or UDP.

SIP uses the Session Description Protocol (SDP) for session and flow control. SDP serves much the same function as H.245 does in H.323. Text based SDP messages called invitations are used to establish compatible media types and pass call parameters such as CODEC, IP address, payload type, and RTP port numbers. SDP is also used to carry session descriptions in the Media Gateway Control Protocol described in the next section. IETF RFC 2327 describes SDP.

SIP is a client-server based protocol. Clients are referred to as User Agents and could be personal computers running VoIP software or VoIP terminal devices such as IP phones. Servers function in three capacities and are referred to as Proxy Servers, Redirect Servers, and Registrar Servers. A proxy server acts as a relay point for a client, forwarding any requests from a user agent or server to the appropriate destination.

Redirect servers inform clients of the network address that will service their call and leave the client to connect the call. Registrar servers function as gatekeepers, maintaining access to directory services. When a user agent logs onto the network, it registers with the registrar. By checking with the appropriate registrar, registered users can identify and locate each other anywhere on the network.

SIP can operate in either proxy or redirect mode as described below. Requiring users to register with the server when they log onto the network enables user mobility. The flexibility afforded by these two configurations contributes to the protocol's scalability. Speed to implementation is also a key advantage of SIP over other protocols.

Figure 6 shows a standard call using proxy mode. Prior registration of user agents involved in the call is assumed. When operating in proxy mode, user agents see all requests as originating from the proxy server.

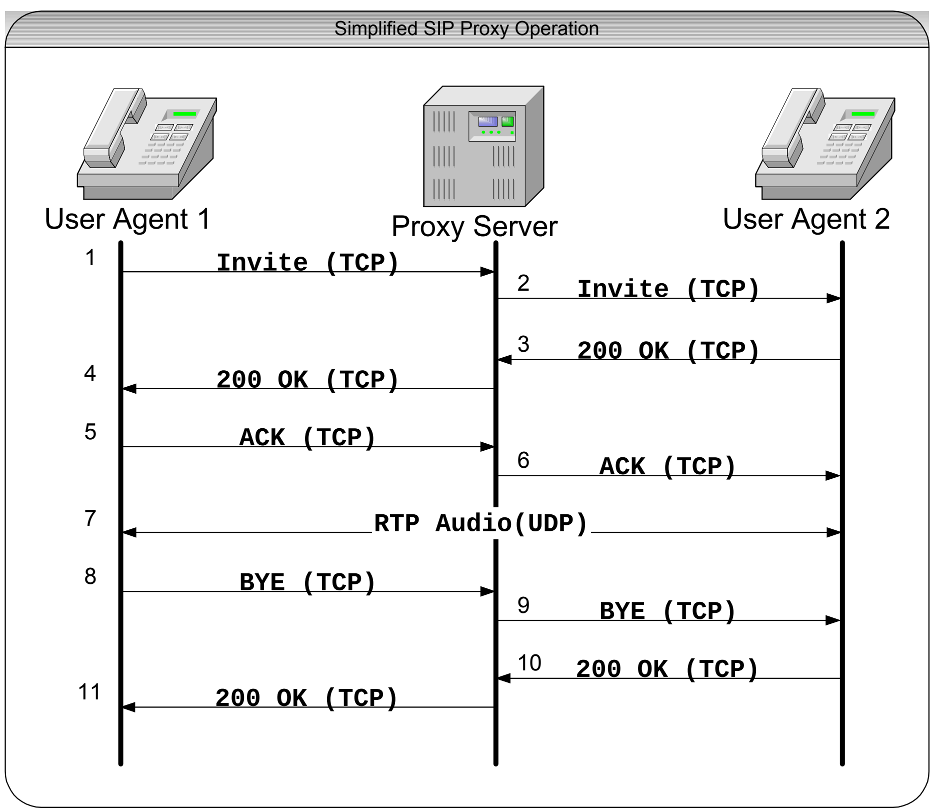

Figure 6. SIP Proxy Mode Operation (After Ref. [2])

Alternately, Figure 7 shows SIP operating in redirect mode. The redirector server supplies the destination client address to the initiator. This address can be the actual user agent address or the address of another redirector server, a proxy server, or the user agent's server. The call initiator then sends all messages to the new address, ultimately establishing an RTP session with the destination.

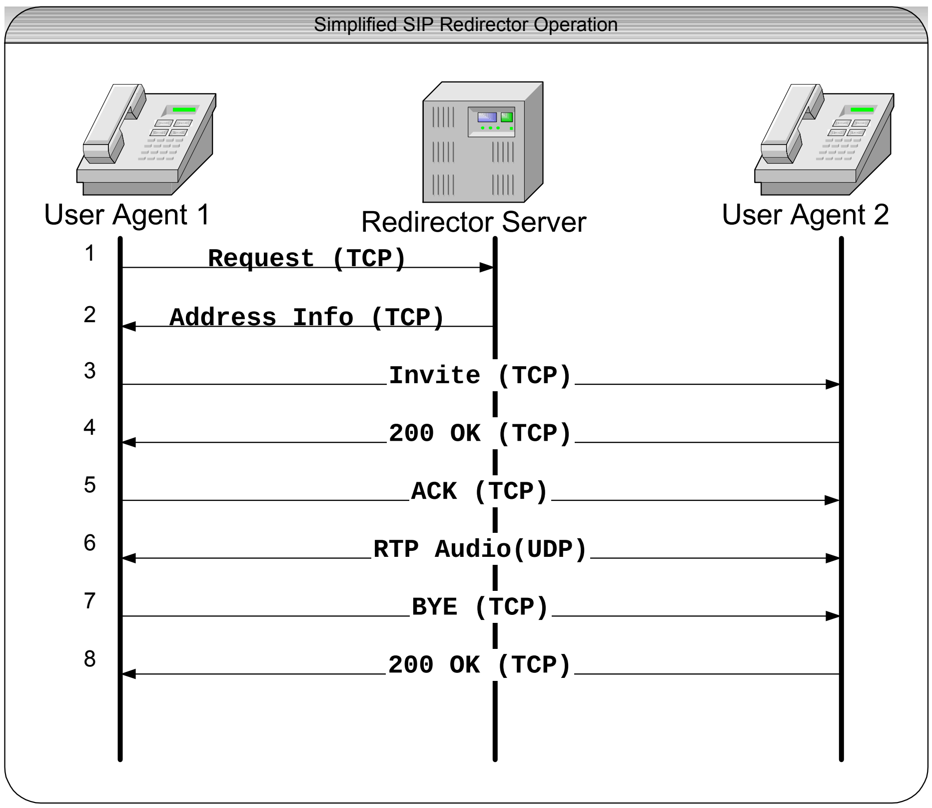

Figure 7. SIP Redirector Mode Operation (After Ref. [2])

4. Media Gateway Control Protocol

Like a number of other emerging protocols, Media Gateway Control Protocol (MGCP) is intended to provide better scalability than H.323. MGCP also provides interoperability between IP networks and POTS networks. However, MGCP's reliance on network addresses to identify endpoints limits its ability to support mobile users. MGCP, as described in IETF RFC 2705 and ratified in ITU-T standard H.248, differs from H.323 and SIP in that it concentrates on the connection between gateways rather than the connection between intelligent end-points. MGCP uses ASCII messages routed over UDP packets to pass control signaling. The principle components of MGCP are Call Agents, Gateways and Endpoints. Endpoints in MGCP refer to any port through which media enters or exits. Endpoints exist at all ports, whether on a Call Agent or gateway.

Call Agents are also called Media Gateway Controllers and serve a similar function as Gatekeepers in H.323. Each Call Agent is responsible for a number of gateways and provides control signaling for calls routed between them. Call Agents also provide the ability to route calls to and from the PSTN. Call Agents use SIP and H.323 to communication with other Call Agents. A common function of the Call Agent is to tell a gateway to set up or tear down a connection between one or more Endpoints.

Gateways are the workhorses of the MGCP architecture. There are numerous types of gateways in MGCP, each named for its appropriate function. Gateways are interfaces between different systems, functioning as translators between media types and formats; they can be connected to POTS telephones, a PBX or a data network. Assigning gateways to more than one Call Agent improves reliability by building redundancy into the network. The types of gateways and their functions are as follows:

- A Residential Gateway connects subscribers to a data network, typically through a DSL or cable modem.
- A Trunking Gateway interfaces the PSTN with a data network and is capable of Time Division Multiplexing thousands of voice channels into RTP packets.
- A Signaling Gateway converts different signaling protocols to interface the PSTN and a data network.
- A Media Access Gateway serves as an intermediary between multiple end users and a Call Agent, effectively removing some of the load from the Call Agent.

Figure 8 illustrates the dialog that takes place during a call setup between two gateways handled by the same Call Agent. There are actually many more control signals passed between the Call Agent and each gateway to establish a single call. For instance, each command to start and stop dial tone would result in a notification or modification of the connection and an associated acknowledgement. A similar exchange takes place for every aspect of the call. MGCP allows for retransmission of lost UDP packets when there is no acknowledgement of receipt but losses still create service interruptions. Some differential service method is needed to prevent loss of MGCP packets and thus minimize service interruptions.

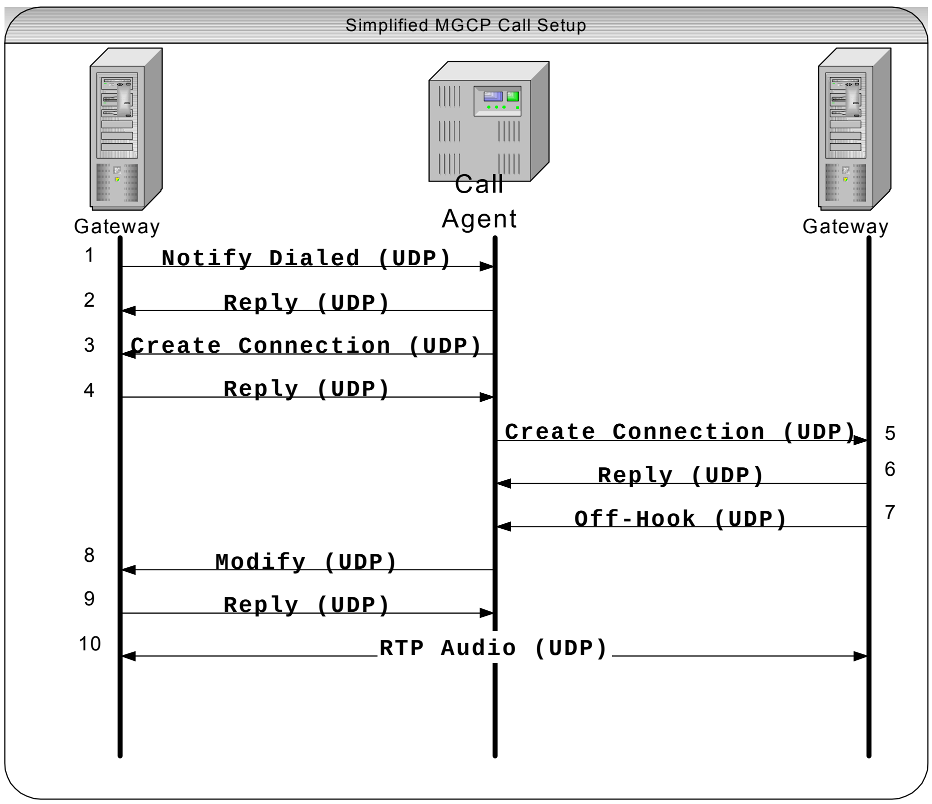

Figure 8. MGCP Call Setup (After Ref. [8])

E. VOIP QUALITY OF SERVICE

When the telephone industry talks about QoS, it is referencing a PSTN phone line. Now when the subject arises, the type of service being referenced must be clarified. Traditional PSTN phones are measured utilizing ITU P.800 recommendation providing a MOS. The MOS is insufficient to measure VoIP QoS; it only measures audio quality. In VoIP many components make up a QoS measurement. ITU G.107 defines "The E-model" for measuring VoIP QoS that provides a single score called a Rating Factor (R). This "R factor" takes into account delay, signal loss, data loss, codec used, and other impairments that occur in VoIP conversations. When an R factor is determined it can be crossed to an estimated MOS. The R factor results in grades of 1 to 99, with less than 50 equating to nearly all users dissatisfied and greater than 90 equating to very satisfied.

1. Delay

Signal delay is made up of several components including Propagation Delay, Transport Delay, and Induced Delay. For VoIP to provide the required QoS, all of the delay components should not exceed 150ms.

Propagation Delay is simply the amount of time it takes a signal to get from point A to point B proportional to the speed of light as it passes through the atmospheric, copper, or fiber optic medium. For example there is less propagation delay from Washington DC to Baltimore than from Paris to Tokyo for any given medium.

Transport delay is the delay induced by all the network components that make up the path from the talker to the listener. Each device that handles the IP packets adds some delay. The majority of devices like hubs and switches induce a relatively constant delay. In routers and similar devices, the delay increases as the amount of network traffic increases. Differential Services and certain protocols can be used to reduce transport delay.

Delays in packet delivery can result in inconsistencies in arrival time, producing a phenomenon called jitter. Delay that is introduced into the system when there is a wide variation in the arrival time of VoIP packets is Induced Delay. Due to the nature of network routing it is possible for packets to arrive out of order at the destination. So, prior to conversion back to analog, received packets are reordered using RTP and held in a jitter buffer to be released at a standard rate of one packet every 125µs.

2. Signal & Data Loss

Any signal transmitted though a medium is subject to signal attenuation. This is a result of absorbing, diffracting, obstructing, refracting, scattering, and reflecting influences. Attenuation is usually expressed in decibels (dB).

When IP packets are transmitted on a network using UDP there is no guarantee of delivery. Therefore, some packets arrive too late for inclusion in the conversion from digital to analog and are discarded. Other packets never arrive at all; the primary reason for packet loss is queue overflow from congestion in routers. For voice communications losses up to 10 percent are not usually noticeable. VoIP typically reproduces the last packet received to fill in the gap for lost packets.

3. CODEC (Compression/Decompression)

When a voice signal is converted from analog to digital form, a CODEC is used to optimize use of bandwidth. A CODEC compresses digital information, which is then put into IP datagrams for transmission over a network. The analog to digital conversion process is presented in Table 2. The CODEC used affects the quality and delay of transmission. When viewing packetization delay in Table 2, note that 30-60 milliseconds delay becomes perceptible to human observation. Delay becomes particularly important when dealing with interactive multimedia.

Compression Method	Bit Rate (Kbit/s)	Frame Size (ms)	Packetization Delay (ms)	Full Duplex Bandwidth (Kbps)	Amount subtracted from R factor
G.711 PCM	64	0.125	1.0	158.93	0
G.729 CS-ACELP	8	10	25.0	46.93	11
G.723.1 MP-MLQ ACELP	 6.3 5.3	 30 30	 67.5 67.5	 43.73 41.60	 15 19

Table 2. VoIP CODEC (After Ref. [2,9])

Currently most gateways support three CODECs shown in Table 2 – G.711, G.729, and G.723.1. Each of these CODECs is defined by ITU-T standards. First, G.711 utilizes PCM voice coding; this is an acceptable form for delivery to a PSTN or through a PBX. Second, G.729 is a low bit rate speech encoder and utilizes the principle of Complementary Symmetry—Algebraic Code Excited Linear Prediction (ACELP).

Finally the G.723.1 CODEC is used extensively in Voice over IP (VoIP), and video conferencing. G.723.1 uses the Code Excited Linear Prediction (CELP) encoding method and can operate on demand at one of two bit rates, 5.3 kbps or 6.3 kbps. The higher rate CODEC is referred to as a Multi-Pulse - Maximum Likelihood Quantizer (MP-MLQ) CODEC and the lower rate as an ACELP CODEC; they differ in the design of the algorithm used.

F. CRITICAL SUCCESS FACTORS FOR VOIP

In this chapter we have discussed the components required for implementation of VoIP, the different protocols, the components of delay and CODECS used. For a VoIP network to provide the required QoS several issues must be addressed. The primary considerations of network performance consist of network delay and reliability, unobstructed flow of UDP packets, and bandwidth requirements.

This chapter provides a basic understanding of VoIP operation and the network-related issues involved. The next chapter explores commercial entities are solving these issues and the predominant VoIP solutions available today. In Chapter Three a vendor is selected and used in a cost benefit analysis with NPS as a model. Chapter Four discusses the limitations of implementing VoIP today. In Chapter Five a lab is set up to simulate the secret portion of ADNS. Transition Management of VoIP is examined in Chapter Six. In conclusion, Chapter Seven examines a possible ADNS implementation of VoIP and areas of possible future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CURRENT VOIP TECHNOLOGY

A. INDUSTRY PROVIDERS OF VOIP TECHNOLOGY

In the competitive industry of telephone service providers there are literally dozens of companies offering VoIP solutions. This chapter will investigate which companies are leaders in the field of VoIP and which company or companies will be best suited to provide a VoIP solution for application in the DoN. The VoIP service providers listed in Table 3 were identified from business financial databases, such as MorningStar and Hoovers Online, and trade journals. When selecting a VoIP service provider many metrics need to be considered. The primary issues need to include interoperability with other VoIP service providers, the financial status of the company, potential for economies of scale, and research and development.

3Comm	Dynamic soft	Pingtel
Alcatel	Juniper	Siemens
Altigen	NEC	Sphere
Avaya	Nortel	Vertical
Cisco	OKI	

Table 3. VoIP Product Vendors

1. Interoperability

Each VoIP solution provider is producing VoIP products that may or may not be compatible with other producers. The incompatibility issues are primarily a result of the different implementations of the ITU-T H.323 and IETF SIP standards. In February of 2002, Network World published an article titled “VoIP Makes Strides. [Ref. 10]” The article addresses an assessment conducted by Miercom Interoperability Testing Labs in which interoperability of seven VoIP vendors was tested. Each vendor volunteered to participate in testing that would prove interoperability between VoIP systems based on the same protocol and between a gateway using SIP and a gateway using H.323. Of the seven vendors tested, only Siemens, DynamicSoft, and Cisco proved successful in the SIP to H.323 internetworking. During the testing conducted only a year prior, gateway-to-gateway interoperability between different vendors was un-achievable as reported by Network World in March 2001 [Ref. 11]. As the growth of VoIP technology continues, and implementation of protocols becomes standardized, the leaders in interoperability will be among those capable of filling the needs of the DoN. Among the three companies that demonstrated successful interoperability, DynamicSoft is a privately held company with limited market share. DynamicSoft declined to provide financial data and, therefore, will not be analyzed further. If interoperability was widely achievable, reliance on a single vendor would less critical and business financials would be less of an issue.

2. VoIP Vendor Financial Status

Since VoIP standards are loosely defined and not widely interoperable across vendors, it is crucial that suppliers of products to the DoN remain in business in the long run. Vendors must be capable of supporting large acquisitions and fleet-wide implementation. Figure 9 shows the seven best sales performers of the companies identified in Table 3 above. Companies with less than one percent of telecommunications market sales relative to total sales of companies listed in Table 3 were not included in the graph. The vertical axis "Percentage of Market" on the graph is the percentage of total telecommunications market sales (which includes VoIP-related sales) in relation to total market segment sales of companies listed in Table 3. Market segment sales were extrapolated back five years based on 2001 sales ratios.

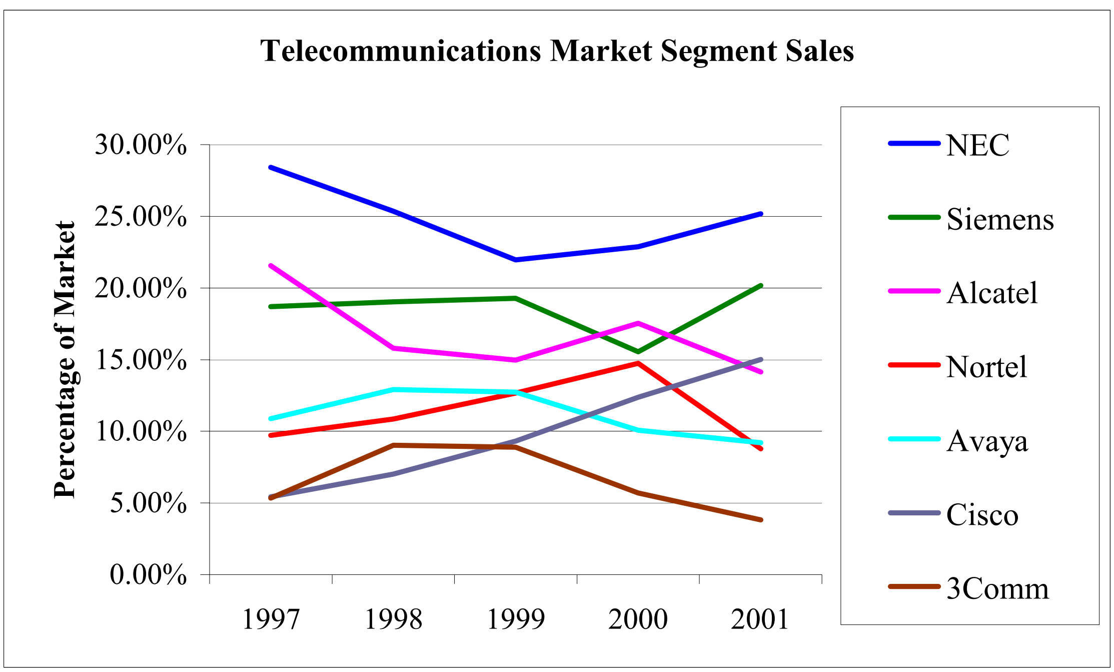

Figure 9. Company Sales in VoIP-Related Departments (After Ref. [12, 13, 14])

The top seven vendors identified in Figure 9 are 3Comm, NEC, Siemens, Cisco, Alcatel, Nortel and Avaya. NEC is a large Japanese corporation with only 7 percent of its total sales in the United States. Contacting the company did not yield more detailed United States sales data. Due to the lack of sales detail, the inability to ascertain where the equipment is manufactured, and the broad corporate segment in which NEC's VoIP-related sales are categorized, NEC will not be analyzed further as a potential provider. A similar argument exists for the French company, Alcatel, which had less than 20 percent of total 2001 sales within the United States. Likewise, Alcatel will not be analyzed further. 3Comm sales for 2001 were below five percent of the evaluated market and have been declining for the past two years. 3Comm's small percentage of market sales precludes it from further analysis.

3. Economies of Scale

Economies of scale are decreases in the marginal cost of production as a firm's extent of operations expands. The ability to leverage this reduced marginal cost should be considered when examining the possible VoIP solution providers. Avaya, Cisco, Nortel, and Siemens all have significant production infrastructure. Examining telecommunications sales and number of employees from Table 4, Siemens and Cisco may have a slight size advantage over Avaya and Nortel. Most of these companies sub-contract out a large portion of production work enabling growth without additional fixed cost, somewhat mediating the larger size of the others.

4. Research and Development

Research and development (R&D) spending is one indication of a company's financial health. If a company has little or no R&D spending, then the company is not investing in the future and probably will not be able to compete in the future. The company that has a healthy R&D program could achieve an advantage over competitors by setting the industry standards for new technology. Nortel invests the largest portion, relative to sales, in R&D at 18.5 percent followed by Cisco, 17.6 percent, Avaya, 7.9 percent, and Siemens with 7.2 percent as shown in Table 4. The company with the best track record of reaping return on investment has to be Avaya. Avaya, a spin-off from

Lucent Technologies (previously Bell Labs), has a history of several decades of success. Past performance is no guarantee of future success, but demonstrates the potential of a healthy R&D program.

Company Name	Total Sales in $ Thousand	Telecomm Sales	R&D Dollars (% of Sales)	Sales Growth 2001	Market Cap in $ Thousand	Number of Employees	Nationality
3Comm	2,821,000	2,284,929,000	535.7 M (19%)	-35.0%	2,033,400	8,165	USA
Alcatel	22,622,000	8,458,529,935	2,552 M (11.3%)	-21.8%	17,274,000	99,314	France
Altigen	9,630	9,632,000	4.85 M (50.3%)	-22.4%	9,084	112	USA
Avaya	6,793,000	5,502,330,000	536 M (7.9 %)	-9.1%	1,956,217	23,000	USA
Cisco	22,293,000	8,984,079,000	3.92 B (17.6%)	17.8%	130,322,776	38,000	USA
Dynamic Soft	4,500	4,500	NA	NA	NA	9	USA (Private)
Juniper	887,000	887,000,000	87.8 M (9.8%)	31.7%	3,740,000	927	USA
NEC	48,579,000	15,059,490,000	3.1 B (6.1%)	6.7%	13,600,000	149,931	Japan
Nortel	17,511,000	5,253,300,000	3.24 B (18.5%)	-42.2%	14,100,000	53,600	Canada
OKI	5,969,763	1,316,929,718	NA	10.5%	NA	25,000	Japan
Pingtel	4,618	4,617,947	NA	NA	NA	35	USA (Private)
Siemens	86,208,000	12,069,120,000	6.17 B (7.2%)	26.1%	54,489,961	461,000	German
Sphere*	13,099	13,098,700	NA	NA	NA	100	USA (Private)
Vertical*	16,016	16,015,500	NA	NA	NA	125	USA (Private)
* Numbers reflect FY 2000 data NA = Data Not Available							

Table 4. VoIP Vendors Key Financial Data, 2001 (After Ref. [12, 13, 14])

B. POSSIBILE VOIP SOLUTION PROVIDERS FOR DON APPLICATION

Assuming that the field of potential providers of VoIP solutions for the DoN is limited to the companies in Table 4, narrowing the possible providers to the top four sellers in the U.S. market reduces the options to Avaya, Cisco, Nortel and Siemens. Each of these companies has unique proprietary implementations of protocols and architectures. Within proprietary networks, unique protocols are used. When traffic exits proprietary networks, it must be translated at the gateway to comply with one of the standards. Conceptually, this process is illustrated in Figure 10. This extra conversion step causes increased latency. The proprietary architectures of each of the four companies and the positive and the negative attributes for each are discussed below.

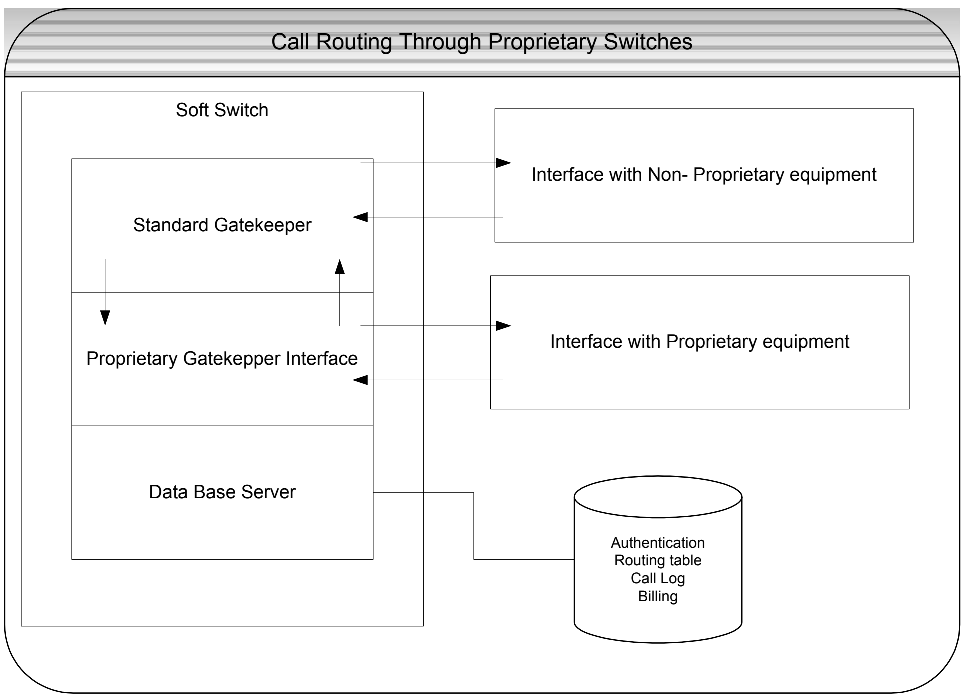

Figure 10. Proprietary Call Routing (After Ref. [6])

1. Avaya ECLIPS

Avaya sells itself as "A leading provider of communications systems and software for enterprises." The solution offered for VoIP is given the name ECLIPS which stands for Enterprise Class IP Solutions. ECLIPS is accredited to Avaya Labs, a new research lab with a 75-year-old heritage from Bell Labs. Avaya plans on a significant boost in capital investment in R&D. The long-term plan is to build a larger R&D community of some 3,000 engineers with Avaya Labs at the center. [Ref. 15 & 16]

The ECLIPS VoIP solution utilizes H.323 signaling. In the spring of 2002 SIP was added to the signaling methodologies supported by Avaya. Two interface cards are used to provide VoIP functionality on the Avaya communications server. These two components are the Control LAN (CLAN) and IP Media processor cards; incremental installation of this card pair provides scalability. Each pair of cards can support between 32 and 64 simultaneous voice calls. Utilizing the G.711 CODEC each call requires 64kps each providing throughput of 64 calls. When a G.729 CODEC is used, each call requires 8kbps but the throughput is halved due to the additional resources needed for compression. The IP Media processor also supports Standard QoS, differential services, and type of service bits needed to prioritize audio traffic across an IP network. The ECLIPS VoIP solution is comprised of Software, Media servers, Media gateways, Communications servers, and Communications devices as shown in Figure 11. [Ref. 16]

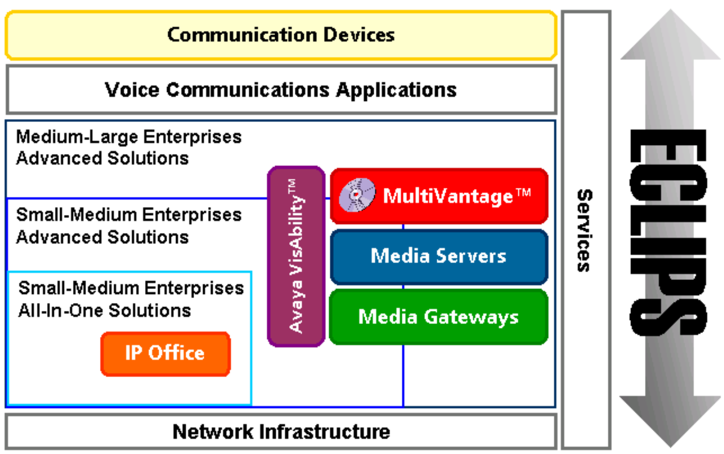

Figure 11. ECLIPS Infrastructure Model (From Ref. [17])

The Software provides for call processing, system management, application integration and enterprise communication networking. The Media server provides centralized call processing that is effective in IP-based and PBX systems. The communication devices vary from traditional analog phones, IP screen phones, IP soft phones, to IP desk phones.

The advantages of Avaya ECLIPS include a proven technology that has the backing of a prestigious research center. H.323 is currently the default standard for VoIP implementation. Incremental network growth also comes in on the side of advantages. A disadvantage has to be the scalability problems associated with H.323. There is no currently available documented third party testing of ECLIPS interoperability.

2. Cisco AVVID

Cisco has created an Enterprise Solutions Engineering (ESE) team to test full-scale deployment of its VoIP products. The network architectures that result are presented as Architecture for Voice, Video and Integrated Data (AVVID) Network Infrastructure solutions. The tested solutions offer increased network performance, potential for expansion, and availability.

Cisco AVVID architectures are based on SIP and are compatible with other standards; some components such as soft phones use H.323. Cisco has been a major influence on the development of SIP and will continue to impact the standardization of this and other VoIP network protocols. Future Cisco products will be tested for backward compatibility and offer the potential to use new protocols as they are developed. Cisco routers and switches are already in widespread use in the DoN and future procurement is planned in conjunction with the Navy Marine Corps Intranet (NMCI). These proprietary devices are the pivotal components of AVVID architectures and offer QoS capabilities that are required for VoIP operation.

The advantages of Cisco AVVID implementation are many, but they come at a price – literally. A recurrent criticism leveled against Cisco is the high cost of its software and hardware. This high cost may be offset by the fact that a large Cisco infrastructure already exists within the DoN.

3. Nortel Meridian

Based in Ontario Canada, Nortel Networks provides one of the possible VoIP solutions. Nortel's enterprise solution is called Meridian and is based on the H.323 protocol. The major components are an enterprise communication server and a communications manager. The Succession communications server, one of the many communication server options, supports up to 640 IP stations per server, allowing for growth as needed. The Succession server can interface with an existing PBX. Nortel's Meridian solution has a little of everything, from Wireless IP Gateway to remote office connectivity. The advantage of Nortel Meridian enterprise products is the ability to provide a complete solution for a data and voice IP networks.

4. Siemens HiPath

Although Siemens is an extensive German company, thirty percent of 2001 sales were from the United States and Siemens Information and Communication Networks, a subsidiary of Siemens, is incorporated in the United States. HiPath is the Siemens Enterprise Convergence Architecture. It is intended for large-scale deployment as a solution for voice and data convergence on an IP infrastructure. HiPath architecture is based on H.323 and is compatible with other standards. Siemens approach is to allow enterprises to pace their migration to VoIP. HiPath is made up of a suite of products including call control servers, IP phones, soft phones, gateways and management software that may be implemented all at once or gradually over time. The products fully support QoS features to ensure voice traffic priority on the network.

As noted earlier, Siemens was one of three companies whose products successfully tested for cross-vendor compatibility. Siemens places great emphasis on large-scale implementation and integration across platforms.

C. THE SINGLE VENDOR SOLUTION

The discussion in this chapter points out the advantage, especially at this early stage of technology development, of sourcing all VoIP products from a single vendor. Advantages include cost savings, tested interoperability, reduced latency, potential for growth and easier system installation and maintenance. All of these advantages are lost, however, if the single vendor used does not remain in business in the long run. Serious consideration must be given to the health of the vendor selected. Factors indicating a sound business foundation and the potential for continued operation are also discussed in this chapter; these factors include total sales, VoIP industry related sales, dollars spent on research and development, and market capacity. Avaya, Cisco, Nortel and Siemens all demonstrate potential for DoN application based on these criteria.

A recent trend at Space and Naval Warfare (SPAWAR) Systems Center has been to purchase Cisco products. Effort is underway to replace all Proteon routers in the ADNS system with Cisco routers. Cisco's AVVID architecture, shown in Figure 12, offers a robust capability backed by a proven vendor.

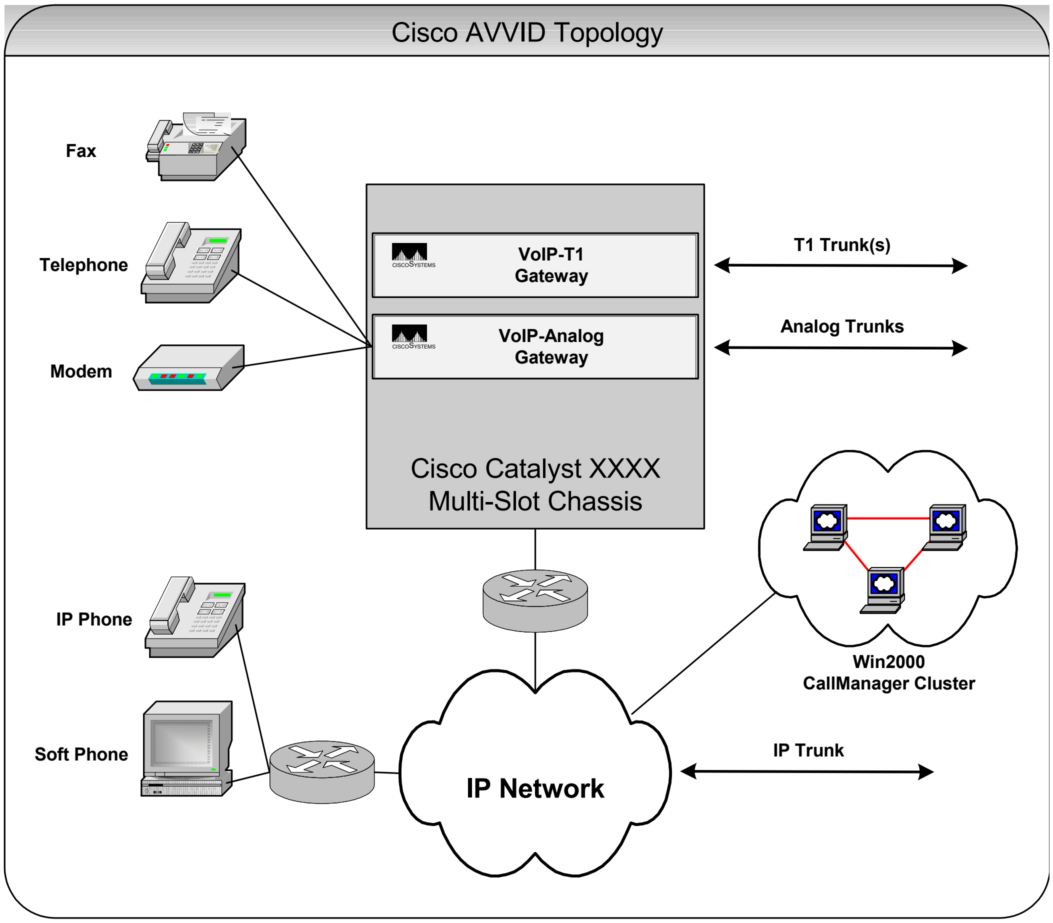

Figure 12. Conceptual Cisco AVVID Topology (After Ref. [18])

The remaining chapters of this thesis will concentrate on implementing a Cisco solution. Reasons for conducting the remainder of the research with Cisco as the single vendor solution include the proximity of the Naval Postgraduate School research facilities to Cisco, the potential for acquiring components from Cisco to build a prototype ADNS network, and the current implementation of Cisco equipment in NMCI. Lastly, the recommendation of our sponsor at SPAWAR is to concentrate on Cisco products. The next chapter will explore the benefits and cost of enterprise adoption of the Cisco AVVID solution.

THIS PAGE INTENTIONALLY LEFT BLANK

III. COST BENEFIT ANALYSIS OF VOIP

A. SCOPE OF ANALYSIS

1. Background

This chapter is intended to provide a model for evaluating implementation costs of VoIP compared to traditional PBX-based phone systems. Three possible options for VoIP implementation are examined. The Naval Postgraduate School (NPS) will be used as a model for this comparison. Currently the NPS phone system has the capacity to support approximately 3,000 end users. This analysis will examine the economic viability of replacing the traditional PBX telephone system with VoIP. Replacement of the traditional PBX telephone system and integrating voice with the data network offer economic advantages, but the costs of this integration can be difficult to ascertain. To determine whether the potential benefits outweigh the costs we will conduct analysis of both tangible and intangible factors. Finally, risk analysis will be used to reach a recommendation regarding adoption of VoIP. For purposes of this analysis, the VoIP implementation options are as follows:

- Immediate replacement of the PBX
- Incremental replacement of the PBX
- Keep the existing PBX system

The first option, replacing the existing PBX system with VoIP in one step, routes voice traffic over an existing data network. Ideally, immediate implementation of VoIP will provide a reduction in total man-hours required to manage two independent networks and eliminate the need to retain PBX support personnel.

The second option involves phasing in VoIP service at NPS over a five-year period. In the interim, IP phones can connect to the telephony network through a digital trunk gateway attached to the multi-service router and through digital loops on the PBX. Maintaining connectivity between the VoIP phones and the analog phones during the migration poses particular technical challenges that service personnel and users need to be prepared for.

The third option is to do nothing at all. That is, keep the existing PBX system and upgrade as it reaches end of service life. With this option, advanced capabilities and potential cost savings of converged networks are foregone in favor of avoiding the costs and challenges of implementing VoIP.

2. Assumptions

The following simplifying assumptions are made to facilitate analysis:

- A VoIP Gateway trunk costs $400 and supports 4 users.
- Call Manager Software licensing costs $150 per user; this is a one-time cost.
- A VoIP phone costs $450 and one support staff can install five phones per day.
- PBX module and handset costs $610 per user. This totals to a capital investment of $1.83 million for 3000 users. Since the PBX system is currently in use, these phones are assumed to already be in place.
- A PBX Switch costs $35,000 and supports seventy-five users. Forty switches are required to support the NPS capacity of 3000 users for a total capital investment of $1.4 million. Since the PBX system is currently in use, these forty switches are assumed to already be in place.
- Annual maintenance costs associated with PBX systems are approximated at six percent of the total capital investment. This percentage is consistent with published industry averages [Ref. 19]. Using this figure, the total annual maintenance cost for 3000 PBX phones and 40 switches is computed to be $193,800.
- Annual maintenance costs associated with IP telephony equates to eight percent of the total capital investment. This percentage is based on industry averages published in Cisco reports [Ref. 19].

- DS-3 leased line for telephony voice service costs $9000 per month. NPS operates the phone system over 16 T-1 lines delivered over a single DS-3 fiber connection.
- The average annual salary of support personnel is $85,000. The equivalent of three man-years for PBX personnel is $255,000. There are 260 productive workdays in a year, so personnel costs are figured to be $327 per staff day.
- A Call Manager server costs $5000. Call Managers are installed in groups of three to provide redundancy and increased reliability.
- A Unified Messaging Server (UMS) costs $20,000 and requires five support personnel staff days to install. The total installation expense for a UMS is estimated to be $1,635.
- Unified Messaging Software Licensing costs $100 per user; this a one-time cost.
- The data network is assumed to be in place and sufficient to support VoIP. The current network trunk consists of an OC-3, capable of supporting the addition of VoIP traffic. The switched backbone has the QoS features needed to enable VoIP.
- Average service life for a PBX switch is ten years.
- A discount rate of ten percent is used for calculating the present value of future year costs.

B. COST BENEFITS

1. Tangibles

Tangible costs are known costs that can be compared among the three options. For this comparison we will examine the cost of installation, maintenance and operation. The assumptions listed in Section A.2 are used in each of the three options that follow. A discount rate of ten percent was used to compute net present value (NPV) for each option.

The NPV of each option was compared at seven years and graphically depicted over twenty years.

a. *Immediate Replacement*

The immediate replacement option financial data is shown in Table 5. In order to support the Naval Postgraduate School's 3000 users, 750 VoIP trunks are needed. All 3000 VoIP phones are planned for immediate purchase and installation, although this number represents maximum capacity; only about 1800 phones are currently in use. Similarly, all 3000 user licenses are budgeted for immediate purchase. Three call manager servers and a single Unified Messaging Server (UMS), which provides the integration of VoIP, Email, FAX and single phone number assignment, are required to support the VoIP system.[5] Maintenance costs reflect VoIP system maintenance only, since the PBX system is discontinued. The NPV of replacing the PBX system with VoIP is $3,423,849 as shown in Table 5.

Initial Costs			**Recurring Costs**		
Hardware			Maintenance	$134,800	
VoIP Trunks ($400 x 750)	$300,000				
VoIP Phones ($450 x 3000)	$1,350,000		PBX Personnel Cost	$0	
Call Manager Servers (3 x $5000)	$15,000				$134,800
Unified Messaging Server	$20,000				
		$1,685,000			
Software					
Call Manager Licensing	$450,000				
Unified Messaging Licensing	$300,000				
		$750,000			
Installation					
VoIP Phone Install	$196,154				
UMS Install	$1,635				
		$197,788			
		$2,632,788			
Year 0	$2,767,588				
Year 1	$122,547				
Year 2	$111,399				
Year 3	$101,275				
Year 4	$92,068				
Year 5	$83,697				
Year 6	$76,095				
Year 7	$69,179				
NPV	$3,423,849				

Table 5. Cost of Immediate Replacement

[5] Single phone number assignment is the ability to assign a phone number to an individual and have that number follow the individual to any location on the network, in the same building or across the country.

b. Incremental Replacement

The incremental replacement option financial data is shown in Table 6. This option replaces PBX phones at a rate of 600 phones per year over a five-year period. The 600 phones require 150 VoIP trunks. All 3000 VoIP phones are planned for purchase and installation, although this number represents maximum capacity and only about 2000 phones are currently in use. Similarly, all 3000 user licenses are budgeted for purchase. PBX personnel are retained until all PBX phones have been replaced. Maintenance costs reflect VoIP system maintenance and PBX system maintenance as it is phased out. The NPV of incrementally replacing the PBX system with VoIP over a five-year period is $5,036,589 as shown in Table 6.

Initial Costs			Recurring Installation Costs (Five Years)		
Hardware			Hardware		
Call Manager	$15,000		VoIP Trunks ($400 x 150)	$60,000	
UMS	$20,000		VoIP Phones ($450 x 600)	$270,000	
		$35,000			$330,000
			DS-3 Leased Line		$108,000
Installation			Software		
UMS Install		$1,635	Call Manager Licensing	$90,000	
		$36,635	UMS Licensing	$60,000	
					$150,000
			Installation		
			VoIP Phone Install		$39,231
			PBX Personnel Cost		$255,000
					$882,231

	Initial	Recurring	PBX Maint	VoIP Maintenance	Total
Year 0	$36,635	$882,231	$84,000	$29,200	$1,032,065
Year 1		$882,231	$67,200	$55,600	$913,673
Year 2		$882,231	$50,400	$82,000	$838,491
Year 3		$882,231	$33,600	$108,400	$769,505
Year 4		$882,231	$16,800	$134,800	$706,106
Year 5		$882,231	$0	$134,800	$631,474
Year 6				$134,800	$76,095
Year 7				$134,800	$69,179
NPV					$5,036,589

Table 6. Cost of Incremental Replacement

c. Keep the Existing PBX System

This option represents maintaining the status quo, that is keep the existing PBX system. The financial data for this option is shown in Table 7. Naval Postgraduate School outsources the operation and maintenance of the PBX through a service contract with Pacific Bell. To facilitate analysis the costs normally included in the lease are detailed in Table 7. Maintenance of the PBX phone system is calculated at a rate of six percent of the total capital costs per year. All PBX associated personnel are retained. The maintenance costs represent planned and unplanned replacement and repair of components. Maintenance costs are calculated for the maximum capacity of 3000 phones although only approximately 2000 are currently in use. All PBX switches will be replaced at the end of service life. The switch replacement cost is budgeted over the ten-year service life of the switch. A total of 40 switches equates to budgeted replacement of four switches per year. The NPV of keeping the PBX system is $4,171,259 as shown in Table 7.

Initial Costs		Recurring Costs			
None		Hardware			
		Replace PBX Switch (x4)		$140,000	
		Maintenance			
		40 switches	$84,000		
		3000 phones	$109,800		
				$193,800	
		DS-3 Leased Line		$108,000	
		Installation			
		4 Switches		$14,000	
		PBX Personnel Cost		$255,000	
					$710,800
Year 0	$710,800				
Year 1	$646,188				
Year 2	$587,405				
Year 3	$534,024				
Year 4	$485,476				
Year 5	$441,336				
Year 6	$401,247				
Year 7	$364,783				
NPV	$4,171,259				

Table 7. Cost of Keeping the Existing PBX

d. Tangible Analysis Results

From a NPV perspective the least expensive option is immediate implementation of VoIP. This implementation presents a seven-year NPV savings of $747,410 over keeping the PBX. Incremental replacement of the PBX leads to a higher seven-year NPV than keeping the PBX. Figure 13 shows that in year eleven the NPV of incremental replacement becomes less than keeping the PBX. Thereafter, NPV is lower for both incremental and immediate replacement than it is for keeping of the PBX. Nowhere in the tangible analysis is service life and replacement cost of VoIP hardware addressed. This omission is due to the fact that call manager and unified messaging server replacement costs are relatively insignificant since most of the initial cost is software and licensing. Replacing or upgrading the servers is accounted for in the VoIP maintenance cost.

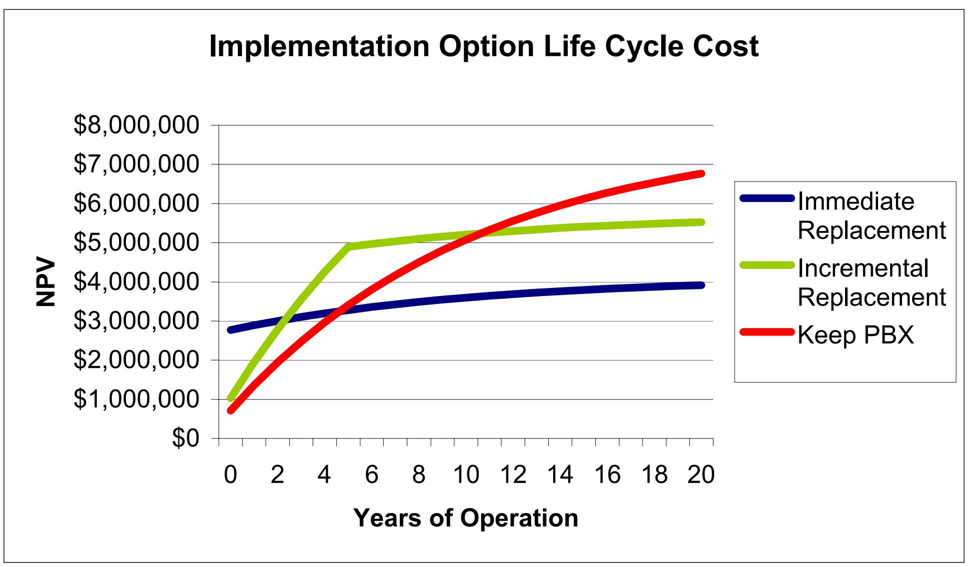

Figure 13. Life Cycle Cost

2. Intangibles

Certain aspects of adopting VoIP do not have actual costs that can be assigned to them. These factors include the need for reliable service, ease of use of the phone system, and the need for secure communications. All of these factors are measurable only through the perceptions and opinions of the system's users, the administrators, and the people responsible for fiscal planning.

In order to quantify an intangible analysis of VoIP versus a conventional PBX, a survey of the Naval Postgraduate School CIO, the Program Officers, the Deans of the four graduate schools, and the Dean of Students was conducted. Survey responses were received from all but three of the graduate school Deans and are presented in Table 8.

Factor	CIO	Code 31	Code 32	Code 34	Code 35	Code 36	Code 38	Dean of Students	Dean GSBPP	Dean SIGS	Avg Score
Low Near-Term Costs (within 2 fiscal years)	4	5	4	3	6	5	2	3	8	6	4.60
Low Life Cycle Costs	8	5	6	2	5	8	2	7	5	3	5.10
Reliability	10	10	8	4	8	10	8	10	9	1	7.80
Security	6	8	5	2	9	10	10	10	4	5	6.90
Ease of Use	10	10	10	5	5	9	10	10	9	2	8.00
Capacity for future expansion	8	7	7	3	8	10	7	8	4	4	6.60

Table 8. Intangible Factor Survey Results

In this survey each person rated the importance of six key factors affecting the decision to upgrade to VoIP on a scale of 1 to 10. Higher values indicated greater importance for the factor in consideration. The following were the factors rated in the survey:

- Low near-term costs. The low near-term cost factor was based on the cost associated with installation and operations for the first two years.
- Low life cycle costs. The low life cycle cost factor was based on the total cost associated with operation and maintenance of the system, from "cradle to grave."
- Reliability. Reliability implies the service is available when it is needed with no unplanned interruptions.
- Security. Security consists of integrity, non-repudiation, confidentiality, and authentication.
- Ease of use. Ease of use is how complicated the system is to use and the features available to the end user.
- Capacity for future expansion. Capacity for future expansion is the ability of the system to grow without upgrading or replacing existing components.

The six factors were assigned weights for each option in the Factor Weight Table, Table 9. Although weights tend to be somewhat objective, values must be assigned in this table with a methodology that can be explained and justified. The weights assigned must be measurable or quantifiable for the intangible analysis to be of any use. To assign the values in Table 9, each factor was compared across the three options and weighted appropriately. Explanations for the weights follow.

Factor	Immediate Replacement	Incremental Replacement	Keep PBX
Low Near-Term Costs (within 2 fiscal years)	4	6	9
Low Life Cycle Costs	9	6	7
Reliability	9	8	9
Security	5	4	4
Ease of Use	9	8	7
Capacity for future expansion	9	8	4

Table 9. Factor Weight Table

For the low near-term cost factor, the least expensive option was given a value of nine and the other values were given proportional values relative to actual cost from the tangible analysis. The same process was used for assigning weights for low life cycle cost; the least expensive option was given a nine and the remaining options were given proportional values based on actual costs.

The reliability factor was weighted a nine for both the immediate replacement and keeping the PBX options since both systems will be engineered for 99.999 percent ("five nines") reliability. The incremental replacement option was given a value of eight due to the potential problems associated with integrating the two systems.

An IP-based infrastructure is easier to add security features to, but neither VoIP nor PBX-based phone systems are inherently secure without additional components. Given that a ten would represent a completely secure system, the security weight for immediate replacement of the PBX was given a value of five. The weights for security in the other two options were assigned values of four due to the incorporation of an inherently insecure PBX. The IP system was assigned a higher security weight than those using a PBX due to the ability to add security features through software and network enhancements such as encryption and tunneling.

A weight of nine was given to the ease of use factor for immediate replacement due to the increased capability offered by convergence of all communications. Ease of use for the incremental replacement option was assigned a weight of eight due to the potential complications associated with a five-year adoption timeline. The weight for ease of use for keeping the PBX was assigned a seven because most users are familiar with its operation. However, PBX systems require separate components for different communication mediums such as FAX, voice, and data; no integration exists across them.

The immediate replacement option was weighted a nine for capacity for future expansion due to the ease with which additional capabilities and phones could be added. Scalability and integration capabilities are far greater for VoIP than for a PBX. Incremental replacement was given a weight of eight due to the delay imposed by the five-year implementation. The PBX option was weighted a four due to the limitations the technology offers in expandability.

The values in the factor weight table were multiplied by the survey averages and the results were displayed in the Decision Table, Table 10. The intangible analysis presented shows that the immediate replacement option best fits the expectations of the users and administrators at NPS. Ease of use and reliability were closely ranked as the most critical intangible factors by survey respondents as shown in Table 8. Both options incorporating VoIP ranked higher in these two areas than did keeping the PBX. Little merit was placed in low near-term costs and low life cycle costs; survey respondents were more concerned with the other factors. The capability offered by VoIP is obviously more desirable than that of the PBX.

Factor	Immediate Replacement	Incremental Replacement	Keep PBX
Low Near-Term Costs (within 2 fiscal years)	18	28	41
Low Life Cycle Costs	46	31	36
Reliability	70	62	70
Security	35	28	28
Ease of Use	72	64	56
Capacity for future expansion	59	53	26
Total	300	265	257

Table 10. Intangible Factors Decision Table

C. RISK ANALYSIS

Uncertainties associated with transition and operations were identified and their resulting costs were quantified through risk analysis. The main risk associated with installing VoIP immediately was identified as an installation delay resulting form a lack of trained installers. The impact of this delay is much greater for option one, installing everything in the first year. The main risk associated with keeping the PBX system is the possibility of having to replace one of the 40 switches before its 10-year service life. The likelihood of this event is assumed to be 50 percent and the cost is high if it does occur. Option 2, incremental implementation, has the potential liabilities of both main risks, although with a smaller likelihood of occurrence.

1. Immediate Replacement Risk

Table 11 shows the risk-adjusted expected cost associated with immediately replacing the PBX with VoIP. The only risk identified is that associated with installation delays that result in additional personnel costs. Instead of installing phones at a rate of five phones per day, each installer is only able to install four phones per day. This would increase phone installation costs by twenty percent or nearly $50,000. Since the chance of this occurring is assumed to be ten percent, the risk exposure is $5,000, resulting in an expected cost for immediate replacement of $3,428,849. This number is used for planning purposes to compare with the risk-adjusted NPVs of the other options. Obviously, if the risk proves founded and installation is actually delayed, total cost would be $3,473,849 represented by worst case in Table 11.

Risk	Probability	Impact	Expected Value
Lack of trained personnel to transition and maintain the system	10%	Installation delay $50,000	$5,000
Total Risk Exposure:			$5,000
Best Case:	$3,423,849		
Total System Expected Cost:	$3,428,849		
Worst Case:	$3,473,849		
Risk Range:		$50,000	

Table 11. Immediate Replacement Risk Analysis

2. Incremental Replacement Risk

Table 12 shows the risk-adjusted expected cost associated with incrementally replacing the PBX with VoIP. The two risks identified were the installation delay covered in the immediate replacement risk analysis above and possibility of one of the PBX switches failing early. Installation delays would occur in one of the five years during which VoIP phones were installed; therefore, the cost impact of the delay would be one fifth of that for immediate installation. This would increase phone installation costs by twenty percent for one year or nearly $10,000. Since the chance of this occurring is assumed to be ten percent, the risk exposure is $1,000. Similarly, the chance of a PBX switch failing early is assumed to be half of what it would be for a complete PBX system, resulting in a risk exposure of $963. The total risk exposure was $1,963 giving an expected cost for incremental replacement of $5,038,552. This number is used for planning purposes to compare with the risk-adjusted NPVs of the other options. Obviously, if installation delays occur and a PBX switch fails early, total cost would be $5,085,089 represented by worst case in Table 12.

Risk	Probability	Impact	Expected Value
Lack of trained personnel to maintain the system	10%	Installation delay $10,000	$ 1,000
PBX Switch fails early	2.5%	$38,500	$ 963
Total Risk Exposure:			$ 1,963
Best Case:	$5,036,589		
Total System Expected Cost:	$5,038,552		
Worst Case:	$5,085,089		
Risk Range:		$48,500	

Table 12. Incremental Replacement Risk Analysis

3. Keep the PBX

Table 13 shows the risk-adjusted expected cost associated with keeping the PBX. The two risks identified were the PBX switch failing early covered in the incremental replacement risk analysis above and the possibility of need for additional capability that the current PBX configuration cannot meet. The chance of one of the forty PBX switches failing early is assumed to be five percent, resulting in a risk exposure of $1,925. The five percent is computed from the designed mean time between failure (MTBF) of 196,000 hours for a PBX. The failure rate is the numerical inverse of the MTBF. The probability of needing additional capacity is assumed to be fifteen percent, resulting in a risk exposure of $6,000. The total risk exposure was $7,925 giving an expected cost for keeping the PBX of $4,179,184. This number is used for planning purposes to compare with the risk-adjusted NPVs of the other options. Obviously, if both risks prove founded, total cost would be $4,249,759 represented by worst case in Table 13.

Risk	Probability	Impact	Expected Value
PBX switch fails early	5%	$38,500	$ 1,925
PBX network requires additional upgrade or repair.	15%	$40,000	$ 6,000
Total Risk Exposure:			$ 7,925
Best Case:	$4,171,259		
Total System Expected Cost:	$4,179,184		
Worst Case:	$4,249,759		
Risk Range:		$78,500	

Table 13. Keep the PBX Risk Analysis

4. Risk Analysis Conclusion

As shown in Table 14, accounting for the risks identified did not significantly change the NPV of any of the VoIP implementation options. The worst-case NPV of immediate replacement of VoIP was still significantly less than the best case for keeping the PBX. Similarly, the worst-case cost of incremental replacement of VoIP still becomes less expensive than the best-case cost of keeping the PBX in the out-years.

	Best Case NPV	Expected NPV	Worst Case NPV
Immediate Replacement	\$3,423,849	\$3,428,849	\$3,473,849
Incremental Replacement	\$5,036,589	\$5,038,552	\$5,085,089
Keep PBX	\$4,171,259	\$4,179,184	\$4,249,759

Table 14. Risk-adjusted NPV Comparison

D. CHAPTER CONCLUSION

The Naval Postgraduate School was used as a model to demonstrate a cost benefit analysis in deciding whether or not to implement VoIP. Based on the tangible, intangible and risk analysis in this chapter, the option of immediate implementation of VoIP would be recommended. This option had the lowest NPV of the three and the intangible analysis results clearly indicated a key stakeholder preference for the functionality of VoIP.

Under certain conditions keeping the PBX could be more cost effective. If the organization's network required significant capital investment to enable the QoS necessary to support VoIP, then this expenditure would need to be included in the cost benefit analysis. Similarly, if the organization was too small to benefit from economies of scale associated with convergence, then keeping the PBX or incrementally adopting VoIP may provide a more economical solution. In both cases the beginning assumptions of the cost benefit analysis would be different than presented here.

Convergence is best viewed as a long-term goal. Upgrades and additions to the network should be made with the goal of enabling VoIP in mind. Any purchases of or enhancements made to traditional phone systems should only be made after analyzing the costs associated with doing so and comparing these costs with those of building the same capability with VoIP. The cost benefit analysis used in this chapter can serve as a model for conducting similar analyses in other commands.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CURRENT LIMITATIONS TO IMPLEMENTING VOIP

A. SECURE VOIP

One of the desired features of a VoIP system is secure voice communication. For communications to be secure, the system would need to include features for confidentiality, authenticity, integrity, and non-repudiation. Where authentication is the ability to ensure that transmissions and their originators are authentic and that a recipient is eligible to receive specific categories of information. Data integrity is the ability to ensure that data is unchanged from its source and has not been accidentally or maliciously altered. Non-repudiation is the ability to ensure the identity of the sender and recipient and that neither can deny having sent or received the data. Confidentiality is ensuring that information can be read only by authorized entities. [Ref. 20]

While secure communication is achievable with VoIP there are several limiting factors to widespread use of this technology. While local area network availability to remote locations can be accomplished through tunneling, this does not provide the desired features for security from node to node. Combining tunneling with key infrastructure enables a secure path from node to node that meets all the aforementioned criteria. A Secure Telephone Unit (STU) combines tunneling and key infrastructure to provide secure communications. Properly implemented, VoIP should be capable of replicating the STU-III functionality on a data network.

The current DoN network backbone from ship to shore is the Automated Digital Network System (ADNS). Network to network connection at the secret level is the native state of ADNS. Unique issues arise when using VoIP with ADNS. The limitations and capabilities will be addressed below.

1. Tunneling

Use of a Virtual Private Network (VPN) provides encryption, authentication of remote users and hosts, and network address hiding. VPNs are usually used to extend private networks over public infrastructure by encapsulating sensitive traffic in IP packets for public routing; this process is referred to as tunneling. VPNs are achieved by Internet

Protocol Security Tunnel Mode (IPSec), Network Encryption System (NES), Tactical FASTLANE KG-175 (TACLANE), Layer 2 Tunneling Protocol (L2TP), Secure Shell (SSh), and Point-to-Point Tunneling Protocol (PPTP). Tunneling of any type introduces latency and creates potential QoS issues. However, it offers a robust and effective means of securing VoIP calls between networks. Tunneling does not provide secure communication from node to node as defined in Section A, but does provide a trusted, encrypted communication path from network to network.[6]

Quality of service (QoS) can be impacted by tunneling. Current tunneling techniques employed in the DoN, particularly the NES and TACLANE used in ADNS, do not copy the ToS byte to the header of the new packet before encapsulation. As a result DiffServ is not enabled and the tunneled VoIP traffic no longer receives priority queuing.

An additional effect on QoS happens when network traffic reaches a level that routers begin to experience buffer overruns; packets carrying the VoIP data can be lost. Consequently, lost packets and network delays lead to interruptions in VoIP conversations and degrade voice quality. Tunneling further impacts QoS by introducing latency. The time required to double encrypt packets is susceptible to CPU speed. Encapsulating the packets at the source and de-encapsulating them at the receiving end adds latency to the call.

2. Key Infrastructure

A Public Key Infrastructure (PKI) enables users of a non-secure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an

[6] For more information on items in this paragraph the following web links are provided:

TACLANE https://infosec.navy.mil/PRODUCTS/CRYPTO/kg-175.html, (April 2002)

FASTLANE https://infosec.navy.mil/PRODUCTS/CRYPTO/kg-75.html, (April 2002)

IPSec http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214037,00.html, (April 2002)

Secure Shell http://www.ssh.com/products/ssh/, (April 2002)

L2TP http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci493383,00.html, (April 2002)

PPTP http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214312,00.html, (April 2002) organization and directory services that can store and, when necessary, revoke the certificates. Certificates can be in the form of software from a centralized authority or a physical device similar to a Fortezza card. A public key infrastructure has the following elements:

- A certificate authority (CA) that issues and verifies digital certificate. A certificate includes the public key or information about the public key
- A registration authority (RA) that acts as the verifier for the certificate authority before a digital certificate is issued to a requestor
- One or more directories where the certificates (with their public keys) are held
- A certificate management system [Ref. 20]

The technology is available now to implement a secure VoIP network that utilizes a key infrastructure. PKI can be used to secure a VoIP phone call with most of the overhead accrued during call setup. A trade off between call quality and security can be made depending on the level of security desired. Interoperability is still an issue among different vendors. Currently no common policy or process is in place to ensure interoperability between vendors of PKI [Ref. 21]. VoIP is not a driving factor in the evolution of PKI; it is driven instead by commercial use of PKI for data transfers and commercial or E-commerce Internet transactions. VoIP will benefit from future technological growth in the area of PKI.

3. Secure Telephone Unit, Generation III (STU-III)

The STU-III is a telephone device in wide use throughout the DoN for conducting secure voice and data transmission over commercial or non-secure networks. SPAWAR San Diego has experimented with using a STU-III to conduct secure voice communications over simulated satellite VoIP link. In the test STU-III calls were packetized with a Quintum A800 VoIP gateway and carried over an ATM network similar to those found aboard ship. A test was considered successful if four out of five calls were connected and maintained in secure mode for greater than two minutes. The minimum bandwidth for a successful test was 128 Kbps. This same network was able to support two STU-III calls, two POTS calls and 50 Kbps of data load simultaneously. At

64 Kbps, no successful STU-III tests were demonstrated. With the scarcity of satellite bandwidth the consensus is that 128 Kbps is too much to dedicate to a STU-III call. The SPAWAR comparison concluded that, "In general, it seems unlikely that any of the successful combinations will be efficient enough to be a viable Secure Voice mode solution. Therefore, it was deemed that this VoIP implementation does not support STU-III secure calls." [Ref. 22]

4. Automated Digital Network System (ADNS)

The Joint Maritime Communications System (JMCOMS) utilized by the Navy and Marine Corps employs ADNS as the backbone. ADNS uses off the shelf protocols, processors and routers to create a robust and flexible networking environment. Internet Protocols (IP), Asynchronous Transfer Mode (ATM) and other products are being adapted from the commercial world. ADNS provides an interface to all RF media from HF to EHF and provides the total throughput for access needed.

Figure 14 shows a configuration diagram for ADNS. The unclassified portion of the system is double encrypted, creating QoS and Bandwidth problems for VoIP. An unclassified VoIP phone call would be layer three encrypted by the NES prior to the secret system router and then it would be layer one bulk encrypted by the KG for the satellite link it would travel over. The overhead for each VoIP packet would become a significant portion of the transmitted signal.

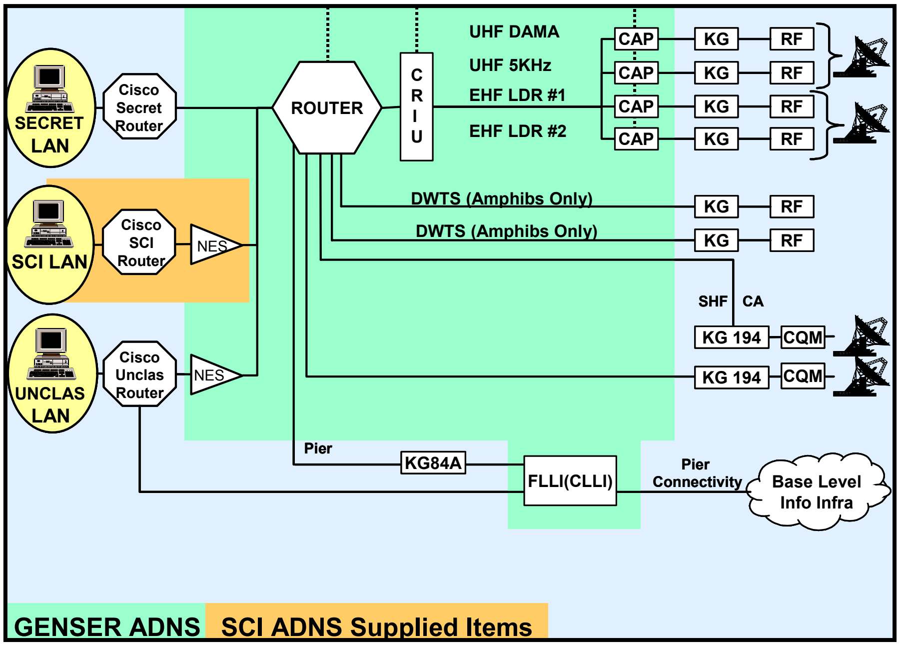

Figure 14. ADNS Configuration Diagram (After Ref. [23])

CODECs at the IP telephony gateway that compress incoming PSTN speech samples generate packets with sizes ranging from 5 to 24 bytes per speech sample. G.723.1 generates a 20 or 24 byte speech packet at 30 ms intervals. Small size packets are subject to a proportionally large overhead when transferred using the Real time Transport Protocol (RTP). The RTP/UDP/IP overhead is 40 bytes (12 RTP + 8 UDP + 20 IP) for a single speech packet. For example, a 20-byte voice packet encapsulated within RTP/UDP/IP has an overhead of 66% [Ref. 2]. Even with this high overhead fifteen VoIP phone calls can fit in the same bandwidth of a single 64Kbps PSTN phone call. When the overhead of double encryption is added to the equation the QoS for the call cannot be guaranteed. This is an area that requires additional research. In the next chapter, VoIP will be routed over ADNS at the system high secret level, thereby avoiding the double encryption issue.

B. TECHNOLOGY ISSUES

VoIP technology is still maturing. Call setup, switching and even interoperability issues are nearly solved. However, there are services that the current PSTN system provides that VoIP vendors are still struggling to emulate. Capabilities that are expected in DoN applications but are not perfected using VoIP include what are referred to in circuit switching as Multi-Level Precedence and Preemption (MLPP) and emergency 911 services. Even silence suppression, which works well to save bandwidth in conventional application, has limitations when used over DoN networks.

1. Multi-Level Precedence and Preemption (MLPP)

The Multi-Level Precedence and Preemption (MLPP) are defined by the ITU in Recommendation I.255.3. MLPP service provides prioritization of call handling and consists of two parts. The first part is precedence, which involves assigning a priority level to a call. The second part is preemption and involves the seizing of resources that are currently in use by a call of lower precedence for a higher-level precedence call in a congested network. MLPP is important to a VoIP implementation because it allow placing prioritization on individual calls, enabling management of limited bandwidth. [Ref. 24]

Currently VoIP systems do not support MLPP. Prioritization of calls in a VoIP network is achieved by limiting physical access to the end terminal. The difficulty in implementing MLPP in an IP network stems from the issue of not being able to preempt a VoIP call that is in progress for a call of higher-level precedence. Industry is actively working to solve the problem of implementing MLPP in a VoIP network.

James M. Polk, a member or the IETF and an employee at Cisco Systems, is the author of a draft IETF standard for implementation of MLPP. This draft standard is still a work in progress. The term MLPP-over IP (MoIP) is used in the document when referring to MLPP in an IP network. This draft MoIP standard attempts to capitalize on as many existing IETF standards and practices as possible. For MoIP to work without interfering with other MoIP networks, the boundary settings must be restricted to a specific domain. For MoIP a domain is defined as everything within the logical IP boundary supporting MoIP capabilities in a single network. A MoIP domain could be a CVBG organized as an autonomous system. [Ref. 25]

MoIP can be broken into several areas of specialization: header marking, routing, signaling and call control, and media. The draft MoIP standard envisions implementation of MLPP services by marking precedence of every VoIP packet in the IP header identification field. Routing will be accomplished with traditional IP routing. Signaling or controlling the precedence/priority end-to-end will be accomplished by using SIP, MEGACO, or MGCP. The mechanism used to set the priority to a communications stream from end-to-end will be differential services or RSVP. [Ref. 25]

2. Enhanced 911 (E9-1-1)

Federal and state laws mandate that Local Exchange Carriers provide Enhanced 9-1-1 (E9-1-1) service to all subscribers, but this is not mandated in Navy shipboard requirements. To enable E9-1-1, PSTN Class 5 switches pass all 911 calls to the appropriate Public Safety Answering Point (PSAP); at the same time, the calling number (called Automatic Number Identification or ANI) and a database link for Automatic Location Identification (ALI) are also provided. Based on the phone number initiating the 911 call, the PSTN switch determines which PSAP should receive the call. [Ref. 26]

There are several unique issues associated with E9-1-1 on VoIP systems. First, VoIP systems provide unreliable location reporting. Since one of the features of VoIP is single phone number assignment and following, no guarantee can be made that the location in the registry is the actual location of the phone. Another issue is one of availability. Ensuring battery backup for phone service during a power failure is a weak point for VoIP. For analog phone systems, power is distributed over the same line as the signal from the switch. Most VoIP vendors have solutions to maintain power at terminals; a harder issue concerning power arises when battery back-up for all the switches, servers, and gateways involved in a VoIP call are examined. The number of often geographically dispersed components needed for a single VoIP call to work requires well-coordinated installation and maintenance of uninterruptible power supplies. A final concern with E9-1-1 in VoIP is the fact that "dial tone" is no indication that E9-1-1 access is available. The gateway to the PSTN can be down but the phone will still work on the IP network. In the event of gateway failure, there would be no indication that emergency services were unavailable until the number was dialed.

Of course, the commercial sector is hard at work trying to solve these problems. Solutions for most of the concerns mentioned above are in development. Automatic Location Identification (ALI) Databases can be implemented in VoIP systems to maintain the location of IP phones as they are assigned a new IP address via Dynamic Host Control Protocol. Additionally, newer IP phones are being built to allow users to enter their location at the terminal. Lightweight Directory Access Protocol (LDAP)-compliant directory applications can be used to ensure access to the stored location information by the PSAP. [Ref. 27]

Most solutions for routing E9-1-1 with VoIP can be categorized as either automated on-net routing or off-net routing. Solutions implementing on-net routing send all 911 calls to a local extension where local security personnel having familiarity with the caller's location can coordinate with public emergency personnel as needed. With the off-net routing solution, the gatekeeper can select the appropriate PSTN Local Exchange Carrier based on the calling number's membership in a calling search space. Calling search spaces can be set up by location of phones. [Ref. 26]

3. Limitations of Silence Suppression

Silence suppression is defined in Chapter 1, Section A1. For silence suppression to offer any bandwidth savings, the sending terminal must have a low enough background noise level to be considered "silent." In environments where background noise is significant, such as aboard ship, the potential advantages of silence suppression are lost. Even when the sender is not talking, the transmitting device will continue to send noise that it determines is loud enough to be significant.

Measures can and should be taken to allow silence suppression to work. Installing push-to-talk buttons on shipboard VoIP phones is recommended as one solution. Push-to-talk buttons are already required on all handsets in classified spaces. Another would be to build a squelch control into the phone transmitter.

C. IMPACT OF LIMITATIONS ON IMPEMENTING VOIP

Tunneling does not proved a secure method of communications from terminal to terminal but with the addition of PKI secure VoIP calls are possible. The STU-III is not bandwidth efficient over a data network; development of another form of secure VoIP connectivity will need to be developed collectively by the DoN and commercial vendors.

The lack of convergence in the current ADNS architecture limits the benefits of VoIP. The topic of secure VoIP over ADNS is an area that requires additional research.

Current limitations to VoIP implementation stem from maturity of technology issues. The best way to address limitations at this point is to stick with a single reliable vendor. E9-1-1 is less of a concern in the DoN since most emergency service personnel are local, relying minimally on public services. In most cases military personnel are notified first and are able to coordinate with civilian emergency support personnel as needed. MLPP is a current capability that must be present in any replacement phone system. Currently, MoIP is under development and should be available in the near future.

THIS PAGE INTENTIONALLY LEFT BLANK

V. VOIP LAB EXPERIMENT

A. LAB INTRODUCTION

The reasons for setting up the VoIP lab were threefold – first, to enhance understanding and knowledge of VoIP technology; second, to test such tenets of VoIP as QoS and convergence first-hand; and third, to better ascertain the applicability of current VoIP technology to the needs of the DoN. Acquisition cost was a driving factor in the lab's design due to budget limitations. The components used were the most capable Cisco VoIP and QoS enabled products that fit within budget constraints. To purchase the hardware and software required for this lab setup would require a budget of approximately $50,000. The test lab set up at NPS capitalized on network components already on campus and generous equipment loans from Cisco Systems and SPAWAR, San Diego. The software package, Expert Observer, was used to monitor the network and generate traffic. A clocked serial cable connecting two routers was be used to simulate the limited bandwidth of a satellite. However, the serial link did not introduce latency that would occur in a connection established through a geostationary satellite.

B. SETUP OF A SIMPLIFIED ADNS ARCHITECTURE

The lab experiment was set up to simulate the secret portion of the ADNS architecture as shown in Figure 14. The hardware configuration shown in Figure 15 was comprised of three primary components, the Afloat Network, the Ashore Network, and a testing/monitoring station (not shown). The Afloat and Ashore configurations had only minor differences. Cisco SP12+ IP phones were used both Afloat and Ashore; two are shown at the bottom of the Afloat configuration in Figure 15. These phones are old models and are no longer supported by Cisco, but they met the needs of this experiment. The two Cisco 2621 routers are shown at the top of each equipment rack. Beneath them are the Cisco 2950 switches used to connect all devices in each network to the router. At the bottom of the Ashore Network the Cisco MCS 7825 call manager is shown. Atop it is an AT8 Analog Gateway that allows access to up to 8 commercial phone lines. The call manager used Afloat is not shown, as it was not rack mounted.

	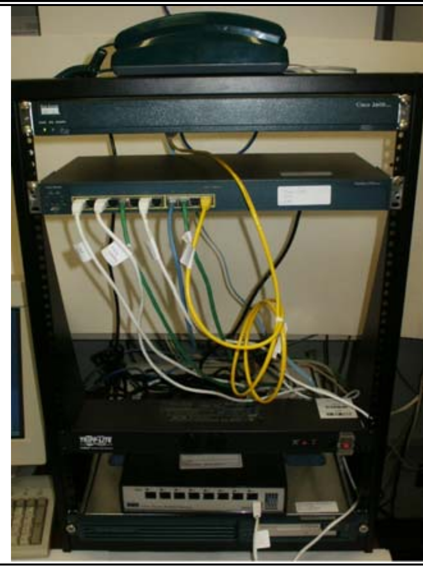
Afloat Network	Ashore Network

Figure 15. Network Equipment

A network diagram of the lab system is presented in Figure 16. Prior to beginning the setup of the lab, planning considerations included an IP numbering plan to support the desired networks and a dial plan for the phones. The IP numbering scheme is shown in Figure 16. Three separate networks comprise the lab, the 10.11.1.X. network ashore, the 10.21.1.X network afloat and the 10.10.1.X network connecting the two over the serial link. The dial plan is shown in Table 15. Standard seven digit numbers were assigned to all phones. The three-digit prefix ashore was 100 and the three-digit prefix afloat was 200. IP phones were assigned extension numbers beginning with zero (e.g., 0001) while analog phones were given extensions beginning with one (e.g., 1001). The plan would easily transition to a real world implementation. The IP addresses in the lab could be changed to IP addresses already assigned in the fleet. The standard seven digit numbers used in the lab could transition easily to actual numbers assigned in the Defense Switched Network.

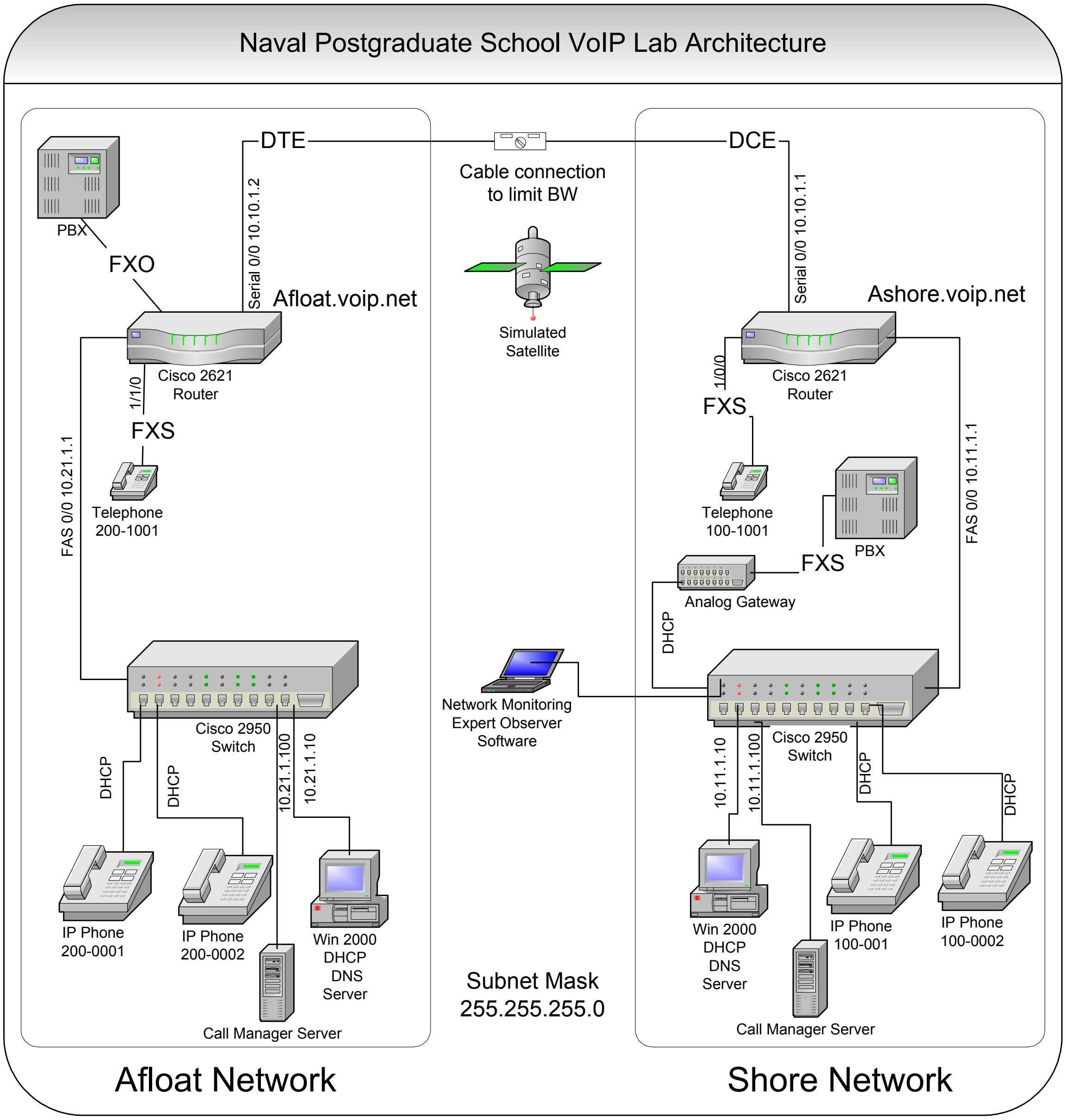

Figure 16. VoIP Lab Configuration

Site Name	Call Manager IP	Directory Number	Intra-site Bandwidth
Ashore	10.11.1.100	200-0001 to 200-1001	2048 kbps
Afloat	10.21.1.100	100-0001 to 100-1001	2048 kbps

Table 15 VoIP Lab Dial Plan

1. Lab Setup

The first step to configuring the VoIP lab was to establish a working IP network. DHCP was used to assign addresses to the IP phones – both afloat and ashore – and the analog gateway on the shore. Static IP addresses were assigned to all network management nodes such as the router ports, servers, and call managers. Once all devices were connected, ping and trace-route commands were used to verify network connectivity.

After establishing a working IP network, the call managers were configured. Each site was designed to operate independently. Two IP phones, one analog phone, and an analog gateway to allow commercial access were registered with the ashore call manager. The ship call manager configuration was similar but lacked the analog gateway. After each location was operating properly as an independent cluster, an H.323 Inter-Cluster Trunk was configured to route calls between them. See Call Manager Setup in Section B.2.d below for details on call manager setup and protocols used.

The final configuration step was enabling QoS on the network. This was done primarily through Command Line Interface (CLI) entries in the routers. Through the use of RSVP and Low Latency Queuing (LLQ), voice traffic was given priority over less time-sensitive data traffic through the simulated satellite link. To prevent high volumes of voice traffic from preempting routing of data traffic, priority was extended to no more than 40 percent of the total bandwidth. Enabling compressed RTP and TCP packet headers over the satellite link further enhanced bandwidth utilization by VoIP. Refer to Section B.2.b for details on router configuration. Full Router configurations can be found in Appendix A. Additional QoS features of precedence queuing and silence suppression features were enabled on the call managers.

2. Network Infrastructure

The Ashore network infrastructure represents a configuration that would appear at a Network Operations Center (NOC). The major components of the Ashore network were a router, a switch, a call manager, an analog gateway, IP phones, an analog phone, and a Windows 2000 server. Traffic destined for the terrestrial network or the commercial Public Branch Exchange would route through the Ashore NOC. This capability was modeled through the use of an analog gateway and accessed by setting a route pattern at call origination points. This solution allows the NOC to route VoIP to a terrestrial IP network or a POTS network.

The lab infrastructure on the Afloat side represents what could be configured aboard a small to medium-sized combatant while allowing the ability to scale for larger units. The major components of the Afloat network were a router, a switch, a call manager, IP phones, an analog phone, and a Windows 2000 Server.

a. Router

The router utilized in the lab configuration was a Cisco 2621. This router served as the interface between the satellite connection and the rest of the network, serving the same role as the "fleet-router" in the Navy fleet NOCs. In this lab a Data Communications Equipment (DCE) serial cable was connected to the serial port of the Ashore router. A Data Terminal Equipment (DTE) serial cable was connected on the serial port of the Afloat router, simulating a connection to a satellite transceiver. Voice Wire Interface Cards (VWIC) installed in the Cisco routers can be connected to an existing PBX via a Foreign Exchange Office (FXO) port or an individual POTS phone line via a Foreign Exchange Subscriber (FXS) port. The Afloat router was configured with two FXS ports and two FXO ports. The Ashore router was configured with two FXS ports. In each configuration the router was connected to the switch through a FastEthernet port.

b. Router Configuration

The Afloat to Ashore satellite link was simulated through the use of a clocked serial link between routers. Using DCE and DTE serial cables and entering the appropriate commands in the router accomplished bandwidth limiting on the serial link. The router connected to the DCE cable provides the clock signal that paces communications over the serial link. Figure 17 shows the commands entered into the ashore router to which the DCE cable was connected. Entering the "bandwidth" command on the serial interface set bandwidth to the same value. The serial link was set up to simulate a T1 link; the closest clock rate to 1.54 Mbps that the router would accept was 1.3 Mbps. This clock rate is a close approximation since overhead associated with maintaining a satellite link reduces actual throughput.

```
interface Serial0/0
 bandwidth 1300
 clockrate 1300000
 dce-terminal-timing-enable
```

Figure 17. Enabling DCE Clocking on the Router (After Ref. [28])

Setting up the analog phone on the FXS port of the router was made relatively easy by the call managers. After adding the router to the call manager as a gateway and setting up the appropriate port with a phone number (see Section B.2.d), the commands shown in Figure 18 were entered into the Ashore router.

```
ccm-manager mgcp
ccm-manager config server 10.11.1.100
ccm-manager config
```

Figure 18. Invoking MGCP on the Router (After Ref. [28])

Resetting the gateway on the call manager then caused an XML configuration file exchange and appended the necessary MGCP entries to the running configuration on the router (see Appendix A). The analog phone was then active and able to send and receive calls through the call manager. The same process was followed to configure the Afloat router, substituting the appropriate IP address of 10.21.1.100 for the Afloat call manager in the "config server" line.

Cisco phones and call managers automatically assign a precedence of five to all RTP voice packets. This precedence is carried in the ToS byte of the packet header. The Catalyst 2950 switch routes traffic by giving priority to higher precedence packets and uses a weighted fair queue to prevent starvation of lower precedence packets.

Similarly, policy maps are used to enable LLQ in the router. Figure 19 shows the commands entered in the router to create and apply policy maps.

```
class-map match-all voice-signaling
  match access-group 103
class-map match-all voice-traffic
  match access-group 102
class-map match-any voip-rtp
   match ip precedence 5

policy-map VOICE-POLICY
  class voice-traffic
    priority percent 40
  class voice-signaling
   bandwidth 8
  class class-default
   fair-queue

interface Multilink1
 ip address 10.10.1.1 255.255.255.0
 service-policy output VOICE-POLICY
 multilink-group 1

interface Serial0/0
 no ip address
 encapsulation ppp
 ppp multilink
 multilink-group 1

access-list 102 permit udp any any range 16384 32767
access-list 103 permit tcp any eq 1720 any
access-list 103 permit tcp any any eq 1720
```

Figure 19. Low Latency Queuing on the Router (After Ref.[28])

Packet recognition is accomplished in the router through access lists that filter traffic by port, precedence, or source IP address; access-lists are grouped by assigning identical identifiers to those that will belong to the same access group. Access group 102 permits all UDP traffic on ports 16384 to 32767, while access group 103 permits TCP traffic inbound or outbound on port 1720. Next, class maps classify traffic as voice or voice signaling based on access groups. A policy map named VOICE-POLICY assigns desired priority and bandwidth to each class map. Voice traffic was given priority for 40 percent of the bandwidth and voice signaling is limited to eight kilobits. The policy map also invokes weighted fair queuing for all traffic. Finally, applying the policy map to the outbound serial port on the router enables LLQ.

Compressed headers reduce overhead on a bandwidth critical link by reducing the header sizes of all packets routed across it. Header compression must be set up on both sides of the link. The commands "ip rtp header-compression" and "ip tcp header-compression" were entered into the multilink interface configurations of both routers.

Entering the command "call rsvp-sync" in the global configuration of both routers enabled RSVP. Once enabled, the router synchronized the RSVP signaling protocol and the voice signaling protocol, allowing 10 seconds for RSVP setup. If a call completes setup within the allotted time, the bandwidth associated with the call is reserved for it.

The final QoS feature configured on the routers involved the creation of a multilink that enabled interleaving of large data packets. Interleaving breaks up excessively large packets into smaller, less bandwidth monopolizing ones that can then be transmitted alternately with the smaller voice UDP packets. Figure 20 shows the router commands that were entered to enable link fragmentation and interleaving.

```
interface Multilink1
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
 multilink-group 1

interface Serial0/0
 ppp multilink
 multilink-group 1
```

Figure 20. Link Fragmentation and Interleaving on the Router (After Ref.[28])

c. Switch

The switch utilized in this lab configuration was a Cisco Catalyst 2950. For larger networks additional switches can be added. No configuration of the switch was required since QoS is loaded in the IOS from the factory. This switch comes with default layer two QoS. The default QoS features include reclassifying of frames based on IEEE 802.1p class of service (CoS) value[7], four queues per egress port, Weighted Round Robin (WRR) queuing algorithm to ensure that low-priority queues are not starved, and strict priority queue configuration to ensure that time-sensitive applications such as voice always follow an expedited path through the switch fabric. [Ref. 29]

d. Call Manager

Cisco Call Manager System Version 3.1(3.a), incorporating component and database management, was used. Operating on a Windows 2000 server platform, call manager administration software controls device management and a SQL database stores details of device configuration. All call manager configuration and administration was accomplished through a web-based graphical user interface. The server component of the call manager had to be configured first. The Ashore call manager was assigned the IP address of 10.11.1.100 and the Afloat call manager was assigned the IP address of 10.21.1.100. The Ashore and Afloat call managers were given the names of "CM-Ashore" and "CM-Afloat" respectively as shown in Figure 21.

[7] For further information on IEEE 802.1p refer to http://www.ieee802.org/1/mirror/8021/docs96/d96n169.pdf, (September 2002)

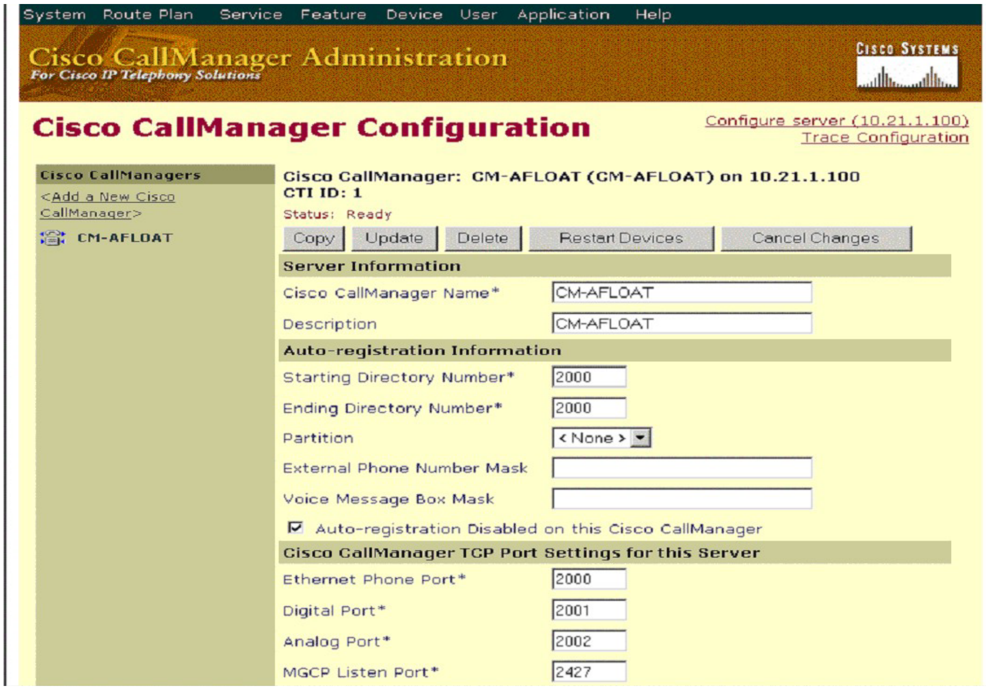

Figure 21. Call Manager Configuration

Next, the regions of the network were assigned. Regions are defined by the administrator and used to set the codec that devices will use to communicate between one region and another. Device pools and gateways are assigned regions. Figure 22 shows the regions set up on the Ashore call manager. Codec G.729 was assigned to communications between Afloat and Ashore to improve bandwidth utilization over the satellite link.

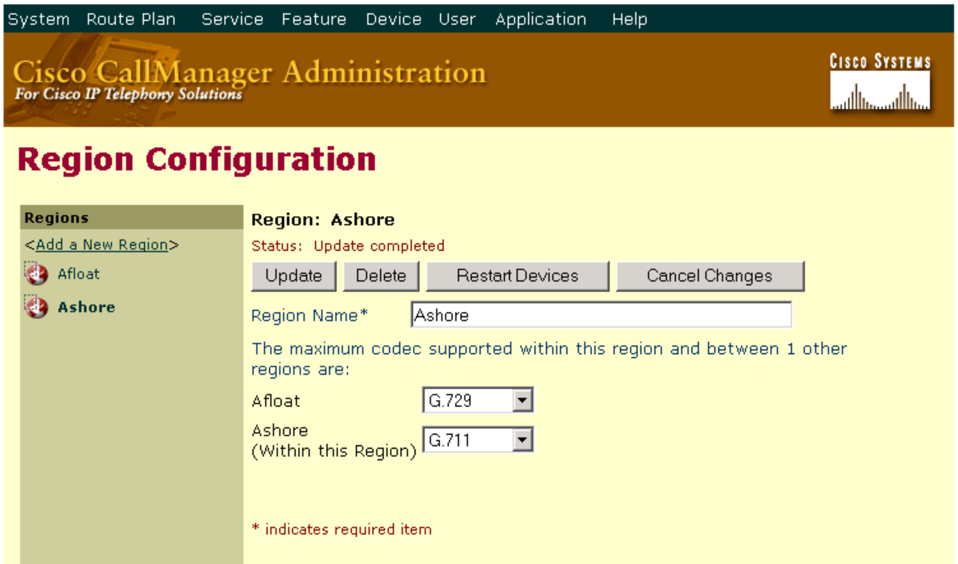

Figure 22. Region Configuration on the Call Manager

Locations define the devices that are locally controlled by the call manager. A location is used to set the bandwidth allowed for use between devices assigned to it. During configuration each device is assigned a location.

Phone devices in the test network include Cisco 12SP+ IP phones, analog phones and an analog gateway. In each network, three phones are used, two Cisco 12SP+ IP phones and one analog phone. The IP phones are added to the call manager in the Phone Configuration menu shown in Figure 23. IP devices are identified by their Media Access Control (MAC) address. The MAC address of each phone is entered, and then the phone lines are assigned numbers in accordance with the dial plan.

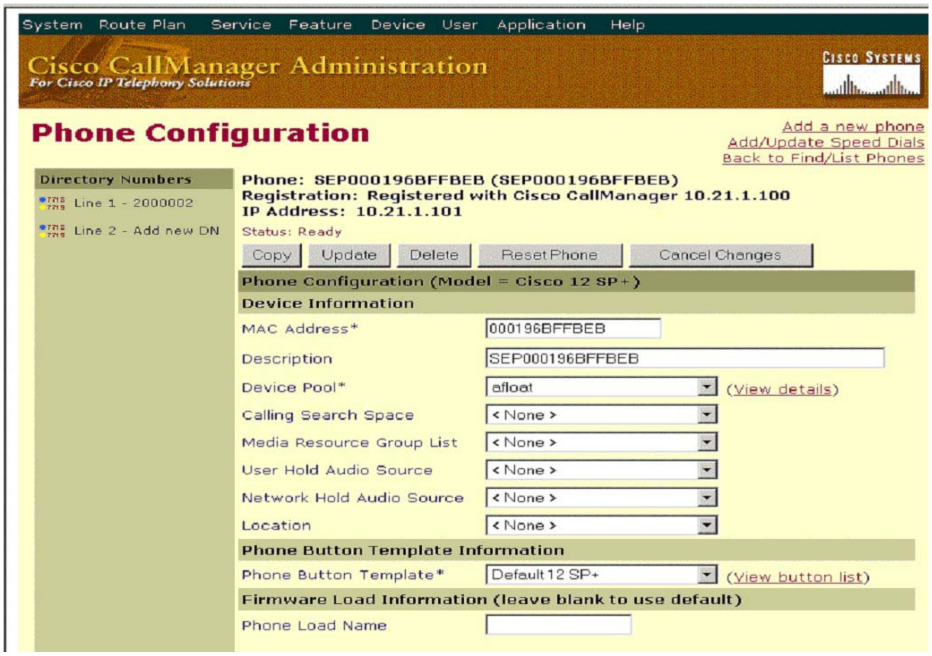

Figure 23. Phone Configuration

Before adding an analog phone, a gateway must first be configured. The gateway for the analog phone is the router to which it is connected. MGCP gateway configuration is shown in Figure 24. After the gateway was added, the endpoints were configured. Endpoints are FXO or FXS ports. Here, FXS port 1/1/0 was activated.

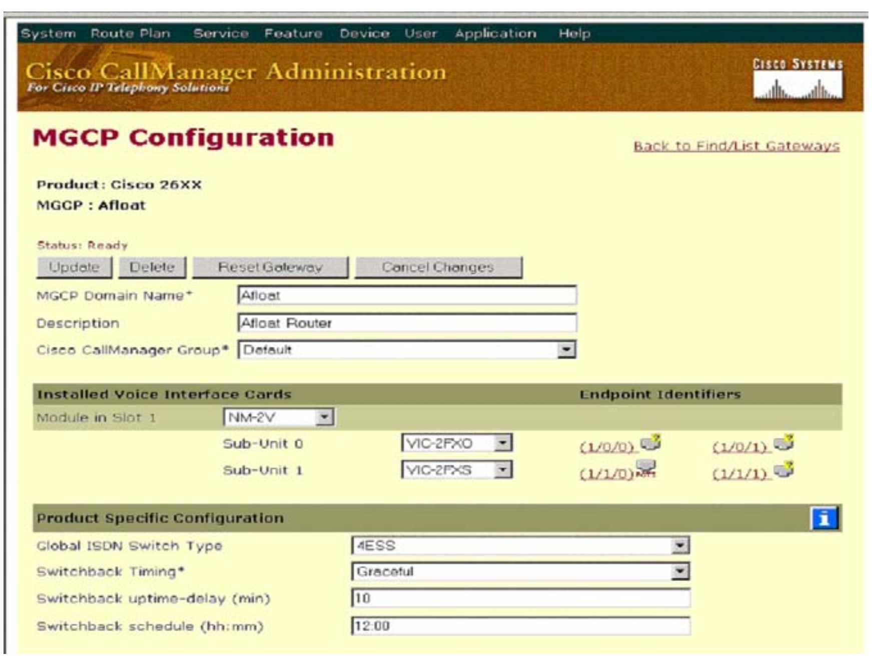

Figure 24. MGCP interface configuration

The AT8 Analog Gateway was configured in a similar way Ashore. The gateway configuration is shown in Figure 25. This gateway allows for eight phone lines to be connected and shared by end users from any location on the network. In the lab the analog gateway was connected to the network at an Ethernet port on the switch.

Figure 25. Analog Gateway Configuration

An Inter–Cluster Trunk was also created in the Device Menu, under Gateway. The required entries include the Device Name, the Device Pool of the destination call manager, the Calling Party Selection, the Presentation Bit, and the Number of Digits. The Device Name is the IP address or name the DNS server recognizes. The GUI for the Inter-Cluster Trunk is presented in Figure 26. The Calling Party selection determines the IP address that will be forwarded with the IP packets. The presentation bit determines if caller ID will be transmitted. The Number of Digits field is the number of digits in the phone number that will be forwarded to the gateway. When the number sequence matching the route pattern that points to the Inter-Cluster Trunk is dialed on a phone, the call is directed to the IP address identified in the gateway. Inter-Cluster Trunks utilize H.323 fast connect signaling to setup and conduct VoIP calls.

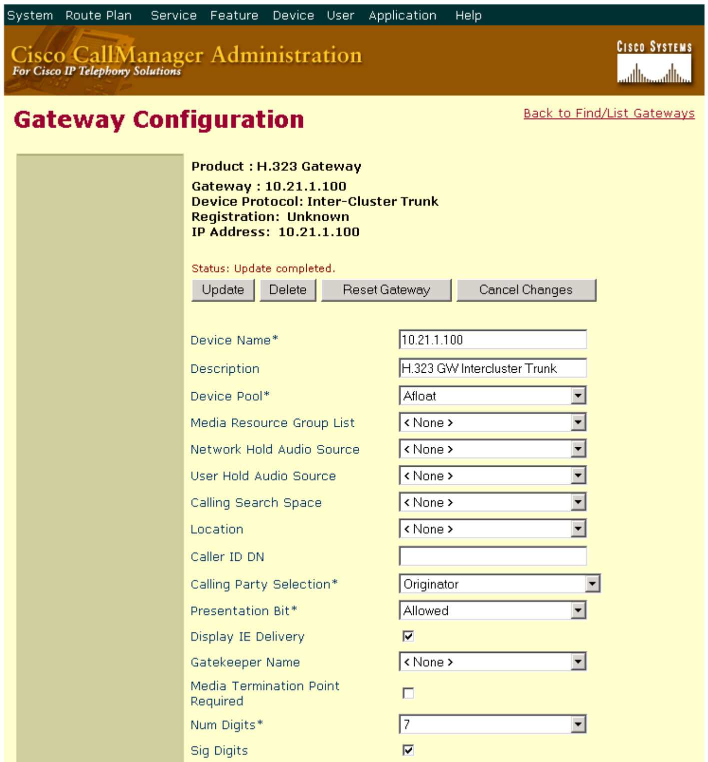

Figure 26. Inter-cluster Trunk Gateway

e. Server

Windows 2000 servers were used in this lab configuration. The main function of the servers was to provide DHCP service, DNS service, and simulated data users on the network. As a server, the call manager is capable of providing DHCP and DNS services. However, this was not done to ensure that the Call Manager was only used to manage VoIP traffic.

C. TESTING AND OBSERVATIONS

Testing of the lab network was limited by the capabilities of available network testing software. Expert Observer software was advertised as a VoIP analysis tool, but in our configuration was unable to recognize any of the H.323 traffic. Expert Observer was not capable of establishing network connections to simulate call establishment or of sufficiently testing the network. A better tool that could be used to test for the bandwidth efficiencies gained by convergence would be Chariot, manufactured by Net IQ. Chariot proved cost prohibitive for this lab.

Limited QoS testing was accomplished by using the Observer software to generate TCP traffic and flood the network until VoIP calls were no longer intelligible. With quality of service features enabled in the call manager the network was able to accommodate a high volume of TCP traffic and still successfully complete VoIP calls.

1. Network Stressing with QoS Control Enabled

To test whether QoS has an impact on VoIP calls, precedence queuing and silence suppression were enabled on both call managers. The network was subjected to 1.1 Mbps of TCP traffic from the Observer traffic generator as shown in Figure 27. To simulate data traffic on the network, 60-byte TCP packets were sent across the serial link from Ashore server to the Afloat server at a rate of 2,000 packets per second.

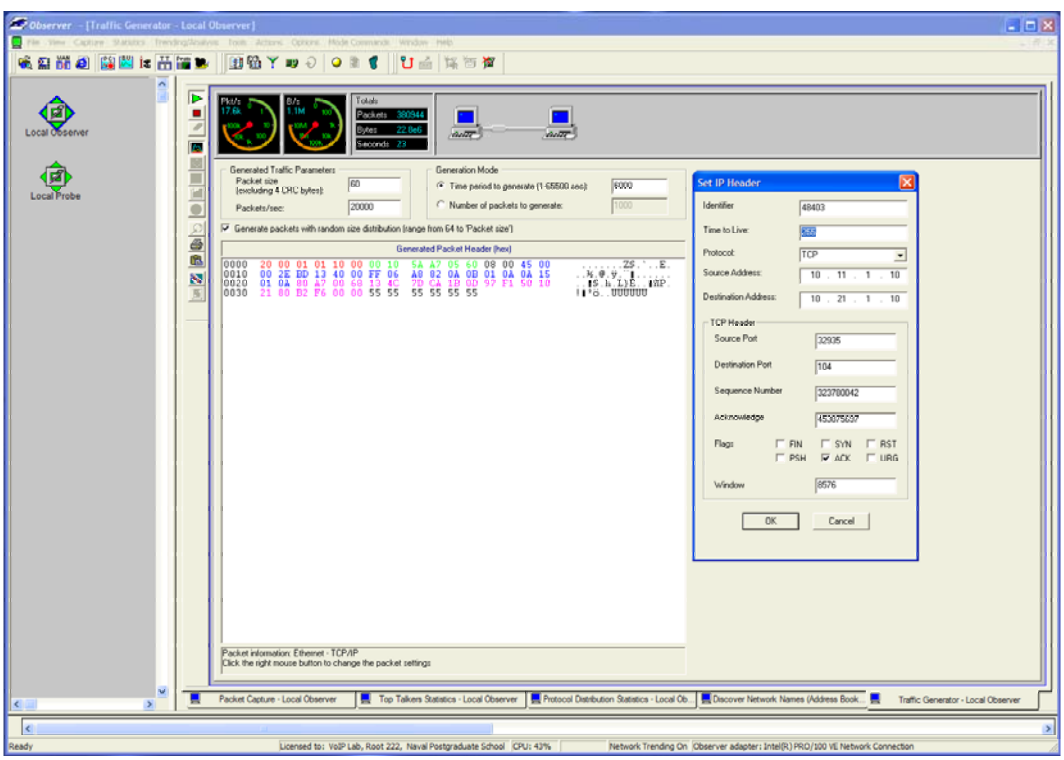

Figure 27. Observer Traffic Generator

At the 1.1 Mbps level of data traffic, VoIP calls were able to setup using MGCP or H.323. Voice quality, however, was poor and H.323 calls terminated within 20 seconds. Multiple calls on the network were not possible. The level of data traffic the network was subjected to was systematically reduced by 100 kbps increments until VoIP performance was comparable to toll quality based on the Mean Opinion Scores (MOS) of the callers. When the level of data traffic was reduced to below 890 kbps, as shown in Figure 28, voice quality for calls became acceptable and calls remained connected indefinitely. At no more than 68 percent utilization by non-VoIP traffic, the 1.3 Mbps serial link with QoS enabled was able to carry acceptable quality voice conversations over all connected phones using both H.323 and MGCP.

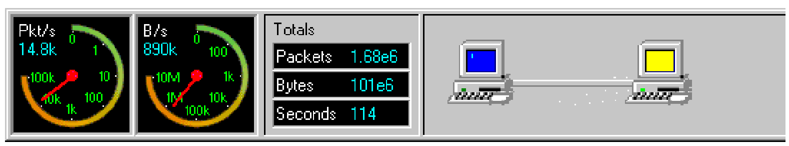

Figure 28. Maximum Traffic Level for Toll Quality with QoS

2. Network Stressing without QoS Control Enabled

Precedence queuing and silence suppression were disabled on both call managers. The network was subjected to 1.1 Mbps of TCP traffic from the Observer traffic generator. 60-byte non-VoIP packets were sent across the serial link from Ashore server to the Afloat server at a rate of 2,000 packets per second. No calls could be established. The level of data traffic the network was subjected to was systematically reduced by 100 kbps increments until VoIP performance was comparable to toll quality. When the level of data traffic was reduced to 788 kbps, call setup was successful but voice quality remained unacceptable. The received signal was broken and calls disconnected after one minute. Further reduction to 705 kbps, as shown in Figure 29, was required to achieve toll quality and indefinite duration on calls. At no more than 54 percent utilization by TCP traffic, the 1.3 Mbps serial link without QoS enabled was able to carry acceptable quality voice conversations over all connected phones using both H.323 and MGCP.

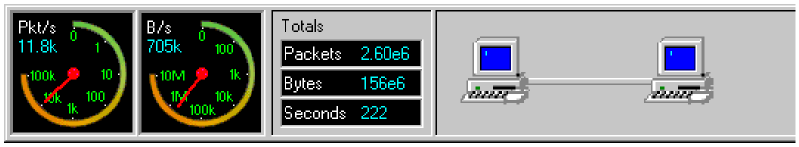

Figure 29. Maximum Traffic Level for Toll Quality without QoS

3. Results of Testing

Figure 30 shows on a logarithmic scale the variance in packets per second injected into the network. On the left of the figure, at time increment 06:12, is the graphical representation of the volume of packets that were achievable with QoS enabled. The level shown on the graph is 14,800 TCP packets per second; packets consisted of 60 bytes. At time increment 06:24 the graph shows that only 11,800 TCP packets per second were achievable without QoS control.

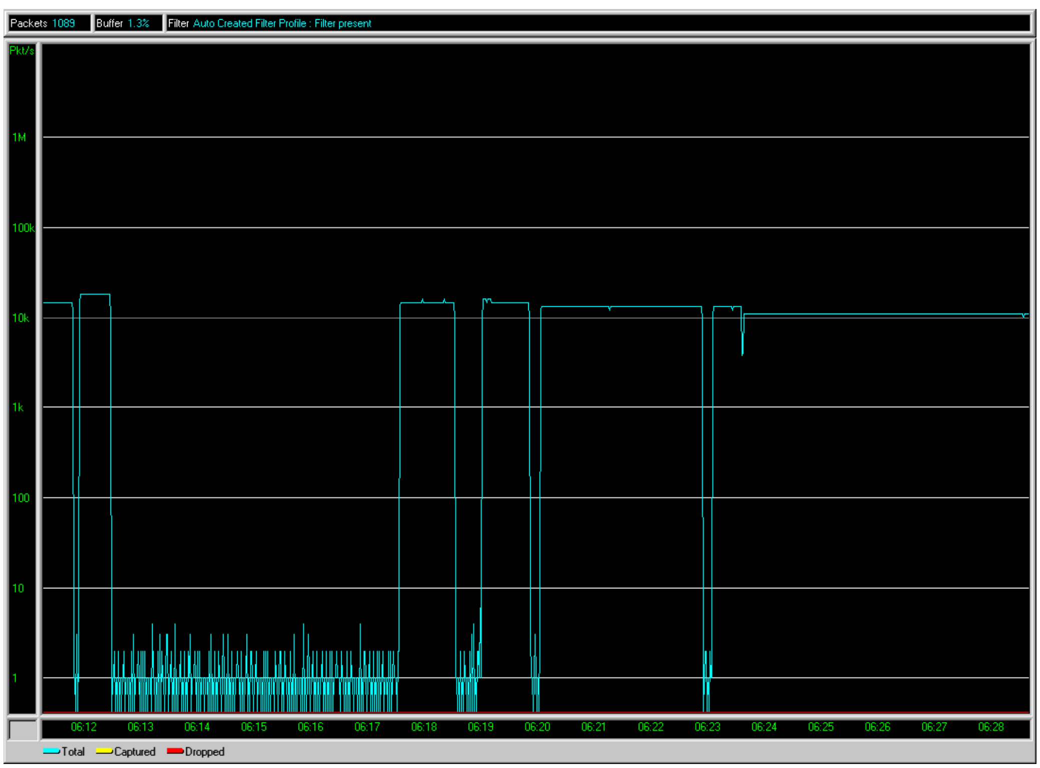

Figure 30. Packet Rate Capture

The level of traffic on the serial trunk greatly impacts the capability of VoIP. If a converged network is to be utilized, then every effort must be taken to maximize the level of TCP traffic while still allowing VoIP. Without QoS enabled TCP traffic could be no higher than 54 percent of the available 1.3 Mpbs serial link before disrupting VoIP. This utilization level was increased to 68 percent when QoS features on the call manager were used. Utilizing QoS resulted in a net gain of 14 percent utilization of available bandwidth or a 26 percent increase in allowable TCP traffic over the simulated satellite link.

VI. MANAGING THE TRANSITION TO VOIP

A. CHANGE THEORIES

The key to a successful change is identifying and selling the problem rather than the solution. While this thesis is primarily on the subject of Voice over Internet Protocol, adoption of this technology was envisioned because of known problems – an old and aging telephone infrastructure in the Department of the Navy, the need for increased efficiency in satellite bandwidth usage, and a potential for reduced cost in personnel and equipment. Today most DoD organizations have two networks installed, a telephone network and a computer network. The telephone network and data network both require dedicated switches, cabling, and personnel. The solution of VoIP is envisioned to reduce infrastructure expense to a single system. VoIP can eliminate the need for a telephone PBX and route all telephone calls over an existing switched computer network. Additionally, VoIP can enhance operational capability by optimizing bandwidth utilization on ship-to-shore satellite links.

Several individuals recognized in the field of modern social psychology provide insight into the process required to implement new technology. These individuals and their theories will be used to explore the process of change. To establish a systemic or whole system view, Peter Senge's System Archetypes will be applied to VoIP. Next, the idea of resistance to change will be addressed by looking at the works of John Kotter and Leonard Schlesinger. Finally, transition management is applied to the change implementation with Kurt Lewin's three-state model and John Kotter's eight-step model.

1. Senge's System Archetypes

Complexity exists in any change. Senge proposes two types of complexity. The first type, dynamic complexity, can only be understood by taking a systemic view of the organization and its environment; only then can the interrelationship between forces driving decisions and actions be understood. The second type is detail complexity, which involves actual steps taken to implement the change. Detail complexity is better understood once you have a firm grasp of the dynamic complexity. The Growth and Under-Investment Archetype presented by Senge best represents dynamic complexity in the system of advancing technology (Ref. [30]). Figure 16 is an adaptation of the Growth and Under-Investment Archetype.

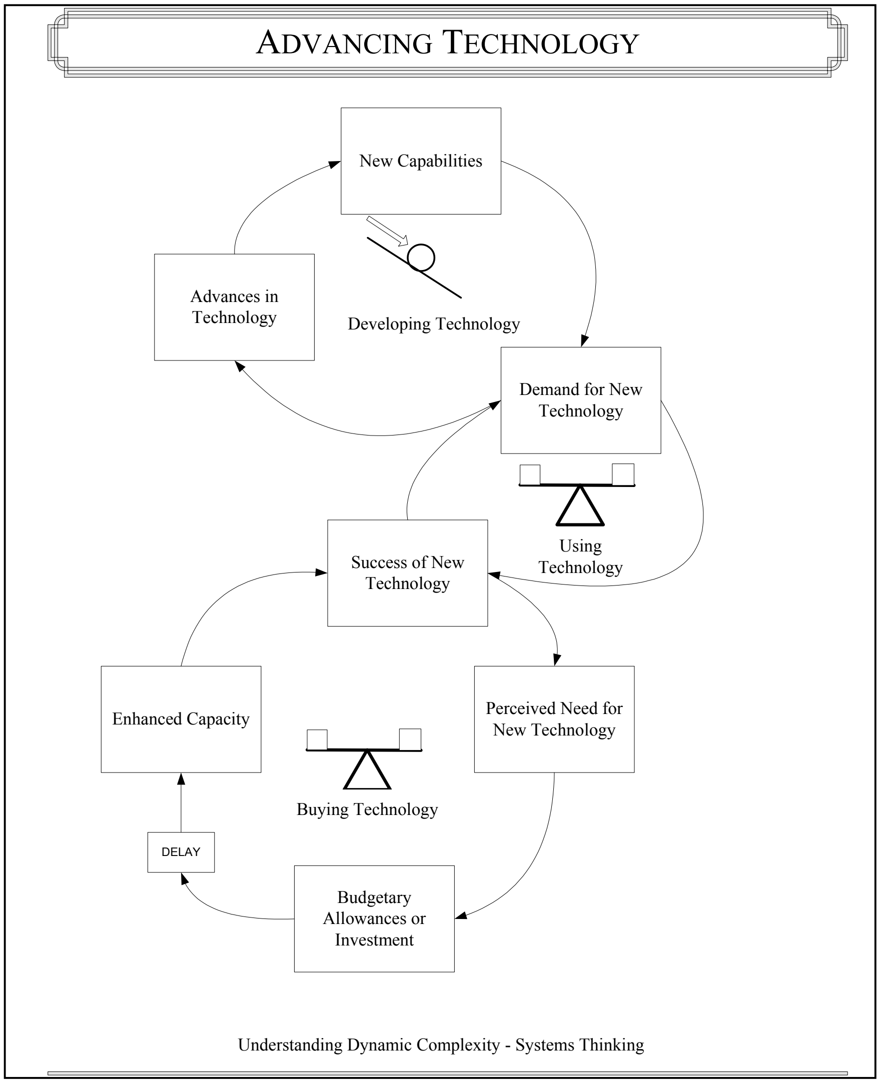

Figure 31. Growth and Under-Investment Archetype (After Ref. [30])

The developing technology loop depicted at the top of the figure illustrates the runaway tendency of developing technology. Advances in technology occur rapidly and unchecked in the absence of some moderating force. The Using Technology loop provides this moderating force. Demand only grows for technology that is successful in implementation. The Buying Technology loop illustrates the fact that there are constraints on the ability of an organization to procure technology.

Budgetary allowances and perceived need both control an organization's desire for new technology. In turn, the organization's desire for new capabilities creates the demand that fuels advances in technology. With this system archetype in place, we are ready to address the detail complexity inherent in the system and discuss the change process.

2. Diagnosing Resistance Using "Choosing Strategies for Change"

Resistance to change is inevitable. In their article "Choosing Strategies for Change," Kotter and Schlesinger state that change often proves to be more difficult in implementation than originally envisioned. Typically, changes take longer and cost more in terms of dollars and morale than managers anticipate. These authors' models will be used to diagnose possible sources of resistance and select a strategy for change that minimizes resistance. (Ref. [31])

Since people tend to view things with their own best interests in mind, they generally resist change that causes them to lose something of value like authority or legitimacy. The authors call this type of resistance "parochial self-interest." Personnel currently manning the PBX switches are likely to surface resistance as a result of parochial self-interest since their positions are effectively terminated. Other personnel likely to surface resistance of this type are the data network managers and workers due to the additional work load and responsibility for implementing the new system. In some cases this resistance may lead to instances of misleading or false attacks on the credibility or plausibility of VoIP.

Another type of resistance that is likely to occur, if it is not prepared for, results from misinformation disseminated due to a lack of understanding of the capabilities and advantages of VoIP. Proper training of key people prior to mandating transition is essential to minimize the effects of misinformation. This process is addressed further below in step 4, Communicate the Vision, of the eight-step model of transition management.

Resistance to change often surfaces as a result of different analysis of the value of the change. If subordinate commands are using different figures to compare costs and capabilities of VoIP to the current system, they are likely to reach different estimations of the best course of action. To prevent competing analysis of the merits and limitations of VoIP, high level commands such as Naval Sea Systems Command (NAVSEA) and Marine Corps Systems Command (MarCorSysCom) should make their analysis widely available. This is best achieved through local seminars and web postings. Feedback should be solicited and considered since new information may alter the official analysis. Never assume all the information is known at the top.

Finally, resistance can result when people are asked to “change too much, too quickly.” Kotter and Schlesinger state that resistance of this type may occur even when the reasons for the change are understood and accepted. Therefore, it is critical to allow time for the training, published analysis, and mandated restructuring to “sink in” before actual implementation. In the case of VoIP implementation in the DoN, implications of this resistance are minimal. Budgetary limitations alone create enough delays in the change implementation to allow the “willing but entrenched” to adjust to the new organizational climate.

In light of the sources of resistance detailed above, the methods that should be utilized to deal with resistance include education and communication, participation and involvement, facilitation and support, and, finally, explicit and implicit coercion. These should be implemented as follows:

Method 1. Education and Communication – Educate subordinate commands and IT managers on the advantages of VoIP adoption. The primary audience for the advantages of a converged backbone, including improved bandwidth efficiencies and reduced support requirements, are IT managers; they will serve as the advocates for VoIP to the rest of the fleet and communicate the transition plan to the users. This training should be started at least three months before planned implementation and materials should be made available online.

Method 2. Participation and Involvement – Subordinate commands, including ships and base facilities, that currently use a PBX should be solicited for their recommendations on how to best transition to VoIP. This solicitation should include technical details on network structure, departmental restructuring, and support. Every effort should be made to include personnel who now run the PBX network.

Method 3. Facilitation and Support – Offer retraining to displaced PBX operators so they can remain in the organization as facilitators of the VoIP network. Pay particular attention to those jobs with skill sets that are readily transportable like field installers and customer relations workers.

Method 4. Negotiation and Agreement – To minimize resistance from the PBX community, offer incentives to PBX network managers if they migrate to the new system.

Method 5. Explicit and Implicit Coercion – To give the change direction and legitimacy, NAVSEA and MarCorSysCom should publish directives mandating compliance with the migration to VoIP. Enough time should be allowed for commands to mitigate some of the resistance through means mentioned above before the VoIP system is actually implemented.

3. The Three State Model: Unfreeze-Change-Refreeze

In 1952, Kurt Lewin first proposed the model of Unfreeze-Change-Refreeze. Edgar Shein expounds on this model in his book <u>Organizational Psychology</u> (Ref. [32]). Basically the model states that for change to be successful, a change must transition through three stages.

- Unfreeze - During this period the motivation for change is created.
- Change - This is the timeframe of actual change. The attitudes and behaviors are developed based on the new information.
- Re-Freeze - This the period where the change is stabilized.

With VoIP some of the unfreezing has already taken place. Many military and government employees are already familiar with computers and telephones. The change has already started to take place with the installation of VoIP in military commands such as the Southern California Offshore Range (SCORE) in San Diego (Ref. [33]). The phone device used by VoIP is similar to a typical desk phone and is no more complicated than any other multi-line phone. This voice communications system solves the problem of limited budgets and advancing technology by eliminating redundant systems and providing enhanced capabilities such as video conferencing and integrated messaging, Along with the users, the people most affected will be the PBX operators and contractors. With the transition to VoIP these jobs will be all but eliminated. Many personnel will be retrained and some will be displaced. The Chief Information Officer (CIO) will gain the additional responsibility of telephone communications.

What are the implications to the social network? The people being displaced will have to be handled with respect and dignity. They have far-reaching influence in the organization and may directly impact on how the new technology will be perceived. The individuals will be retrained for other jobs; individuals with the proper skill set can be retrained for jobs within the network department. Within the network department itself, the CIO will have to ensure that there are enough personnel to handle the increased workload and they are properly trained and competent to not only manage the existing Local Area Network (LAN) but also operate the new telephony technology. This will ensure constructive interactions between the network department and the other departments and users, ultimately leading to positive attitudes toward the new technology.

The change step involves the actual implementation of the system, which must be accomplished quickly. There is not a lot of time for anxiety once the decision to implement has been made. As long as an adequate switched data network is in place, an entire contingent of several hundred phones can be operational in a short period of time. The VoIP phone allows a user to move the phone to any location on the network without a technician changing the wiring or reprogramming a switch. The expedience of the installation and the ease of use will develop new attitudes and behaviors towards the phone system. As a result of using the new technology people's roles will change and a new social network will evolve.

As when Cortez burned his ships after arriving in the new world to prevent any thought of turning back, once the change has been made to VoIP there is no returning to a PBX based phone system. Once the capabilities of the new phones are learned the transition will be total and the oft-anticipated problem of new things learned not fitting into a person's total personality should be limited. Long-term acceptance, or refreezing, is virtually assured. Similarities between the new system and the old will ensure users' adoption of the new technology.

4. Eight-Step Model

Another widely accepted model for change management is the eight-step model, advocated by John Kotter. Even though the Department of Defense is not a for-profit business, many of the attributes do apply to technology implementation in the DoD.

Step 1 – Establish a sense of urgency. Immediate need for adoption of this technology is best achieved by touting the potential monetary savings possible by combining LAN and Private Branch Exchange (PBX) networks. Once again, the key is selling the problem. Establish a directive mandating that all new construction and upgrades to phone systems in the DoD must be justified by cost-benefit analysis compared to VoIP.

Step 2 – Form a powerful guiding group. For the Navy and Marine Corps this system has the interest of SPAWAR, NAVSEA, MarCorSysCom and managers of NMCI. These organizations will provide the guiding impetus for implementation, as they possess the bureaucratic authority and technical expertise to direct action.

Step 3 – Create a vision. This includes the vision of a VoIP phone that can be used anywhere on the NMCI network assigned to each individual. The phone number assigned would stay with the phone without the person calling knowing whether the recipient is in Washington, DC or Pearl Harbor, HI. Each VoIP phone could also be equipped with email and limited web browsing.

The application of this vision to the ADNS architecture offers significant improvements in utilization of limited satellite bandwidth between ship and shore, ultimately leading to a converged IP-based backbone. Tactical communications ashore can benefit from convergence as well by eliminating unnecessary redundant installation, thereby reducing the command and control footprint. Installation of a converged tactical network would require fewer personnel, need less hardware and cabling, and allow a reduction in the logistics train supporting it.

Step 4 – Communicate the vision. Publish the capabilities of this system in DoD magazines and editorials such as SIGNAL magazine published by the Armed Forces Communications and Electronics Association (AFCEA) and CHIPS magazine published by SPAWAR, Charleston, SC. Exposure within the telecommunications community will familiarize members with the new technology. Additionally, and perhaps more importantly, training regional managers (e.g., MARFORPAC, SURFLANT, SUBPAC) and key members of the social network (e.g., communications officers, network and telephone technicians, and Electronic Material Officers) on the capabilities of the new system will have a far-reaching impact in the DoN. Favorable impressions of VoIP technology and its utility instilled in these individuals will perpetuate throughout the organization.

Step 5 – Empower Others to Act on the Vision. In the DoN, directives provide the empowerment to accomplish assigned tasks. These directives remove obstacles to the change. With the direction of NAVSEA, obstacles to adoption of VoIP will be limited to the programming of money for the system. Before VoIP can be implemented fleet-wide, components connected to a secure network must be certified to operate at the appropriate classification level. Contracts such as Indefinite Delivery, Indefinite Quantity (IDIQ) vehicles need to be put in place to allow agencies to purchase necessary VoIP equipment.[8]

Step 6 – Plan For and Create Short-Term Wins. Implement the system in a high profile command first to set the example. This example provides the model for other commands to emulate. One possible venue for fielding VoIP is through a CNO-sponsored initiative. By the direction of the CNO, Commander, Operational Test and Evaluation Force (COMOPTEVFOR) is responsible for operational test and evaluation of new systems of acquisition category (ACAT) I, II, III, and IVT. COMOPTEVFOR has a pilot program called SmartShip that allows rapid prototyping of commercially available technology aboard ship.

Another possible route to implementation is through the Commander, Third Fleet (COMTHIRDFLT). COMTHIRDFLT Instruction 3430.2B outlines the procedure for

[8] For further information regarding IDIQ contracts refer to http://web.deskbook.osd.mil/default.asp, (May 2002)

getting new technology onboard the USS Coronado, the Navy's Sea-Based Battle Lab (SBBL). Sponsorship, possibly from SPAWAR, would be required for funding and operational support of the testing.

Once the technology is proven, each unit or location that installs VoIP moves the DoN closer to total adoption. Each installation produces a short-term win.

Step 7 – Consolidate Improvements and Produce Still More Changes. Obviously all the implications of implementing a new system are not known from the onset. Any command and control advantages that are discovered as the system becomes widely used will need to be published. Due to the fact the technology continues to advance, each improvement in this technology will be implemented at each phase of installation. Liaison between industry and acquisition professionals that will contract installation of these systems will be required to ensure the best value and the latest technology for the dollar.

Step 8 – Institutionalizing new approaches. As the traditional POTS became part of every day life, this new technology, too, will become commonplace. When lessons learned are received, NAVSEA and MarCorSysCom will review them for relevance to operations. Each significant lesson learned will be implemented DoN-wide by directives.

B. SUMMARY OF MANAGING CHANGE

VoIP implementation has the characteristic of involving adoption at two distinct levels within the DoN, on the ship-to-shore backbone and within a deployable force such as an Amphibious Ready Group (ARG) or Battle Group (BG). The process of implementing VoIP differs for each. Adoption of VoIP in the backbone is where the real bandwidth usage optimization addressed in this thesis occurs; VoIP installation at this level involves the Navy Computer and Telecommunications Area Master Stations (NCTAMS) as shown in Chapter 5. Call setup and routing must link with shore infrastructure at the NCTAMS. This means that successful VoIP adoption on the satellite trunk through ADNS can only occur through direction from a higher command with authority over both ship and shore infrastructure. Installation of VoIP across the multi-system boundaries inherent in the current ADNS architecture necessitates direction from a higher level of command authority than exists at the NCTAMS or at the ship type commander.

Clearly, the adoption of VoIP by the Navy and Marine Corps involves a complex change process with many potential sources of resistance. Proper management of the change from concept inception to final fielding is critical to a successful transition. Much research has been conducted in the field of managing change and applying some of the results of this research to the implementation of VoIP is a logical step. By diagramming the systemic view we are able to evaluate the probable sources of resistance. From the result of this diagnosis we have identified five methods of minimizing resistance and creating a smooth transition. Applying the transition management approach to organizational change results in specific measures to follow for successful adoption of VoIP.

VII. EXPLOITATION OF EXISTING VOIP TECHNOLOGY

A. TECHNOLOGY ACCEPTANCE

In this chapter an implementation of VoIP is proposed. First, the challenges of adopting a new technology are addressed. These challenges result from a lack of industry-wide interoperability and the fact that this new technology has not been perfected. There are features of traditional POTS that have not yet been incorporated into VoIP.

Does the VoIP technology available today provide value to the DoN? Yes. Even with this still developing technology there are fiscal advantages and efficiencies to be gained from VoIP. VoIP promises to be a widely accepted technology in the future. The issues of efficient use of bandwidth over choke points, cost savings gained from a common infrastructure, reduced cost associated with toll calls and the merger of the phone with the desktop will keep adoption of this technology on the path to ubiquitous use. In conclusion, this chapter proposes areas of possible further research including expansions on the lab configuration from Chapter Five.

1. Ensure a Reliable Vendor

The emergent state of VoIP technology creates a market in which many small companies compete. As VoIP technology continues to mature the companies that provide the equipment merge with other companies or fail all together. Typically it is the smaller companies that fade away as the market consolidates. This alone should be enough to limit selection of VoIP service providers to companies that can support an enterprise level installation. The Navy should take a lesson learned from the Proteon router that was installed in ADNS in the late 1990s. The manufacturer of the Proteon router no longer exists. The Proteon router was selected because of its strong multi-cast capability. However, a larger view of the industry was not taken. Now the Navy is replacing the Proteon routers with Cisco 3500 series routers. The fact that equipment installed aboard Navy ships or fielded with the Marines may be in service for more than a decade requires long-term support. When the DoN migrates to VoIP technology for widespread use an analysis similar to that in Chapter Two is recommended. Selecting an industry leader is critical to long term support and interoperability, eliminating mistakes like the Proteon router.

2. Sometimes the Answer is No

Not all networks would fiscally benefit from a VoIP installation. As with any business decision the issue of payoff must be addressed. Therefore, any deployment of VoIP or similar technology should be preceded by a cost benefit analysis similar to the one presented in Chapter Three. Prior to allocating further funding to Plain Old Telephone Service installations, policy should mandate that the initiating command conduct a cost/benefits analysis of VoIP installation.

There are other issues that may preclude the adoption of VoIP. Installation of VoIP requires the existing network to meet minimum bandwidth and QoS requirements. Although a cost benefit analysis may indicate that upgrading the network is fiscally prudent, there are additional issues with the technology that must be considered.

a. Capability Set Limitations

Adopting VoIP as a replacement to traditional PBX systems means giving up some functionality. The lack of support for Multi-Level Precedence and Preemption (MLPP) in VoIP is still being resolved. Adoption of VoIP at this point means accepting the loss of a current capability. Additionally, no new terminals for implementing secure voice with VoIP have been certified through NSA. VoIP does not support current terminal devices such as the STU-III efficiently.

b. Protocols Still Maturing

While core standards for VoIP have been developed, implementations of these standards are varied and often incompatible. In most cases products from different vendors utilizing a common protocol such as H.323 will not communicate with each other. Vendors have proprietary implementations of standard protocols as well as protocols of their own. For instance, Cisco uses H.323 to communicate through gateways and Skinny Client Control Protocol (SCCP) to communicate between Cisco devices.

B. POSSIBLE FLEET VOIP ADNS CONFIGURATION

One of the unique configuration requirements when considering implementation of VoIP in the ADNS architecture is that every unit must stand as an independent entity. A typical enterprise VoIP design would set up call managers on a network with one call manager as primary and at least one other as an alternate. Devices such as IP phones are registered with a call manager; the call manager need not be local. In such a configuration all call request packets would travel to the call manager to identify the device being called and then make the connection to the destination device. Having call managers in remote locations may not be an issue in a terrestrial network where bandwidth is abundant and connectivity is always maintained, but aboard ship, system design cannot allow a phone call between the ship administrative department and the executive officer to go across a satellite link for call setup. This issue is resolved by creating a call manager cluster at each location.

The recommended cluster configuration for networks supporting less than 2,500 phones consists of three call managers. One call manager would serve as a publisher and Trivial File Transfer Protocol (TFTP) server from which all devices would download configurations and settings, a primary call manager, and a backup call manager [Ref. 34]. This is a plausible configuration for call manager clusters installed aboard fleet units. To make the system more economical, smaller units with 500 phones or less could eliminate the call manager serving as a publisher. Cisco routers numbered 2621 and higher are capable of acting as a limited back up or redundant call manager, supporting 25 to 50 phones. This feature is called IP Keyswitch and is only compatible with newer model IP phones. [Ref. 35]

To communicate with another independent call manager cluster the call manager must know the IP address of each call manager cluster it will communicate with. In the test lab an outgoing H.323 Gateway Inter-Cluster Trunk was configured each way between the Afloat and Ashore call managers. Expanding this configuration to a task force requires that each cluster be configured with N-1 Inter-Cluster Trunks, where N is the number of independent clusters on the network. These clusters would be interconnected in a typical star topology. As shown in Figure 32, the total number of

Inter-Cluster Trunks, referred to as ICT's, in this network would be N(N-1). Each link represents two Inter-Cluster Trunks, one from each end. A total of 30 trunks are depicted in this diagram. A hypothetical route pattern is depicted beneath each ship number. As an example, Ship 1 would have a unique Inter-Cluster Trunk assigned to five possible route patterns, 2XXX, 3XXX, 4XXX, 5XXX, and one to the NOC that included everything else (except local 1XXX numbers).

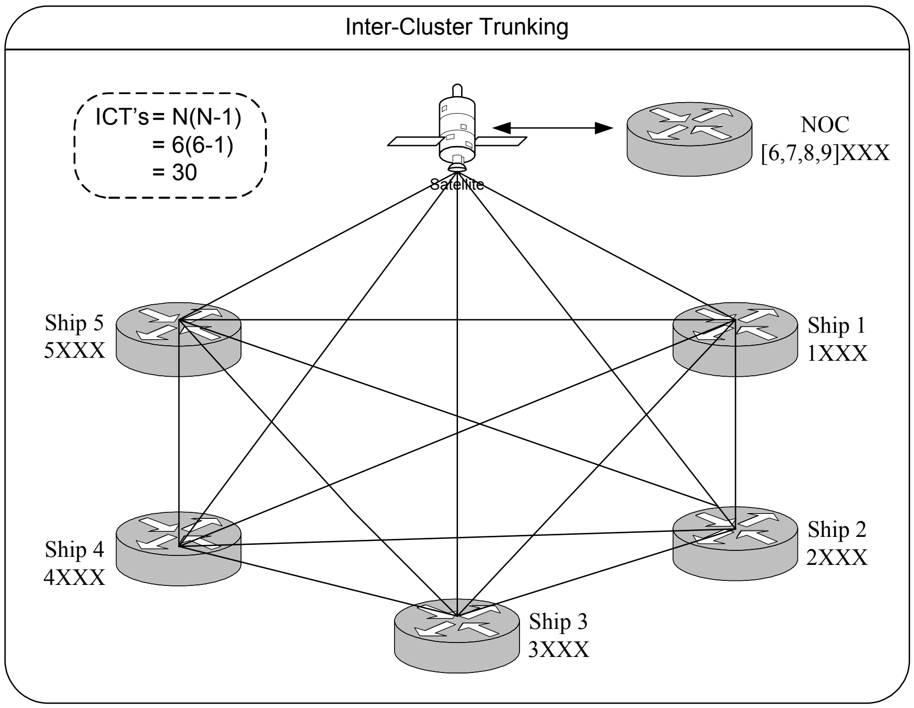

Figure 32. Inter-Cluster Trunk Topology

The configuration illustrated above has several advantages over an open architecture that is centrally switched. It enforces strict adherence to a dial plan while remaining fully configurable. With coordination the network is scalable and dynamic, allowing units to be added and deleted as required. Furthermore, loss of one cluster on the network does not affect the functionality of those remaining. Doubling the number of trunks and assigning two to each link can achieve Inter-Cluster Trunk redundancy.

Setting up a network such as the one in Figure 32 would require a high degree of coordination. All IP addresses must be predetermined and known to each cluster. This is achievable through standard communications plans and messages. Current Navy fleet configurations already have each CVBG organized as an autonomous system.

Supporting the VoIP implementation discussed here would require some preparation and training on the part of support personnel. The learning curve experienced in setting up the lab at NPS should not be duplicated. The additional duties associated with configuring and maintaining the VoIP components of the network need not result in an overwhelming increase in workload for the network personnel already in place. A contractor or tiger team would install the system and configurations could be prepared ahead of time and loaded when needed.

Inter-Cluster Trunking is one solution using Cisco products. Each company offering a VoIP solution has its own variation on system design and implementation. This is an example of one viable option illustrating how VoIP could be adopted in a fleet environment.

C. QUESTIONS FOR FURTHER RESEARCH

The network configuration presented in Chapter Five offers areas of additional testing that were not explored in this thesis. In the lab the satellite link was simulated; sending the traffic over a real satellite link would provide more realistic test data. Further tests include the use of a more robust testing suite to better analyze network performance and bandwidth utilization. The use of SNMP to gain visibility of the network at the routers and switches would enhance traffic analysis. Testing the network by establishing multiple TCP and UDP connections between endpoints would provide more realistic network stressing than did packet flooding using Observer.

Research conducted on this thesis has revealed several areas of interest that warrant additional exploration. While it has been shown that QoS control is critical to successful implementation of VoIP, what forms of QoS to employ is uncertain. Further investigation of the impacts of QoS on DoN specific applications is needed to determine which QoS components should be used on network links such as ADNS. For example, RSVP is time sensitive and differential services may offer better QoS control over a satellite link.

Follow on research could be done to build onto the ADNS model used in the test lab in Chapter Six. An expanded network topology could be set up to include tunneling unclassified traffic over the secret trunk and breaking the unclassified data out through TACLANEs. When the overhead of double encryption is added to the link budget, call setup and QoS cannot be guaranteed. Expanded network configuration should also include latency that is inherent in a satellite link. Such latency can be induced at the router. A possible expanded network configuration is presented in Figure 33.

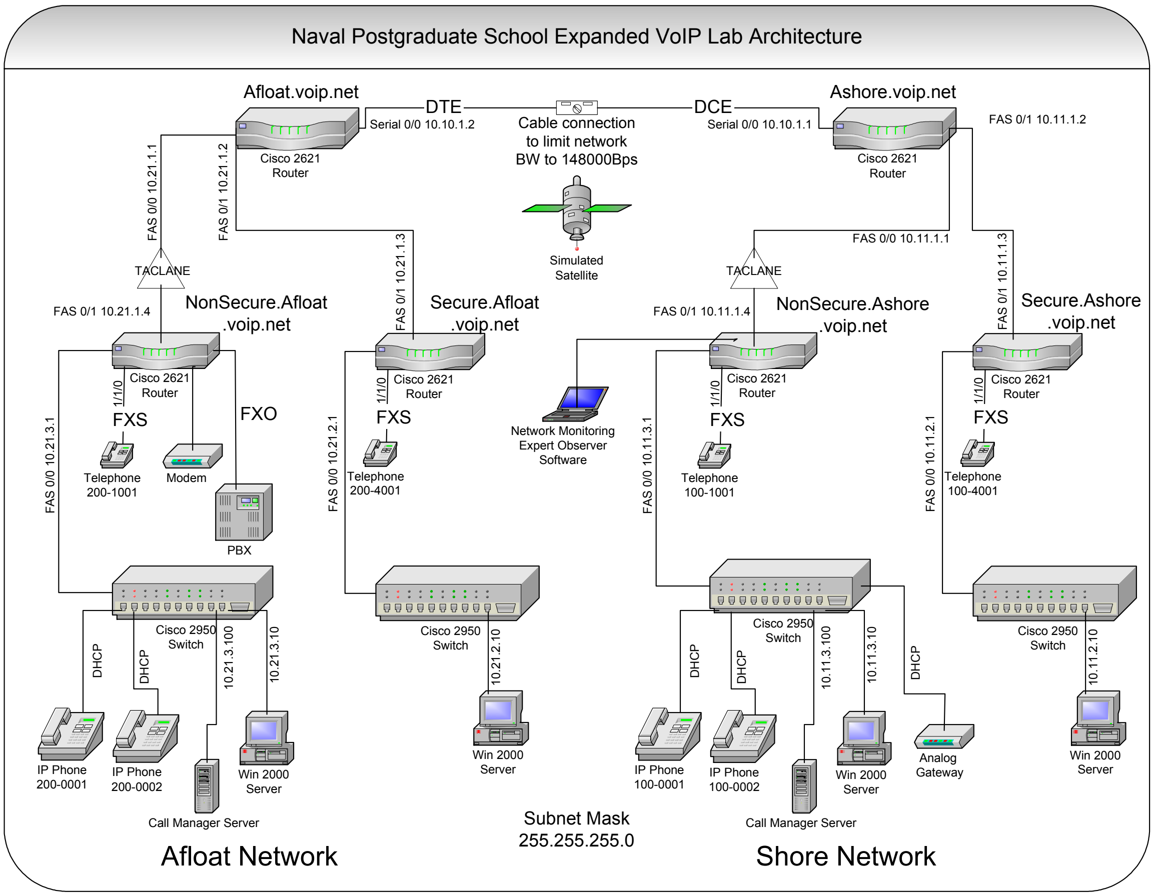

Figure 33. Possible Expanded Network Configuration

Improved methods of network monitoring should be found to generate, capture, and evaluate data regarding convergence and bandwidth utilization. Simultaneous generation of TCP and UDP traffic could be done to test throughput before and after convergence. Software packages such as NetIQ Chariot promise to fulfill these requirements but in the case of Chariot the price approaches $30,000 per license. Acquiring the software is only the first step, as there is a learning curve associated with using testing software.

D. PLANNING FOR CONVERGENCE

Convergence of different modes of information exchange onto a common IP backbone is ongoing and inevitable. VoIP is just one step in that direction. Even if VoIP is not the immediate answer for voice exchange, planning for future adoption is prudent. Network analysis tools should be used to test new components and system configurations for VoIP compatibility prior to adoption. Network upgrades should be made with enabling convergence of voice and data networks in mind. Issues that must be addressed are QoS, throughput, and compatibility.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

AFLOAT ROUTER CONFIGURATION

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Afloat
!
enable password voip
!
ip subnet-zero
!
no ip domain lookup
!
class-map match-all voice-signaling
  match access-group 103
class-map match-all voice-traffic
  match access-group 102
class-map match-any voip-rtp
 match ip precedence 5
!
policy-map VOICE-POLICY
  class voice-traffic
    priority percent 40
  class voice-signaling
   bandwidth 8
  class class-default
   fair-queue
!
voice call carrier capacity active
!
voice service voip
 h323
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
voice class h323 1
 h225 timeout tcp establish 3
!
ccm-manager mgcp
ccm-manager music-on-hold
```

```
ccm-manager config server 10.21.1.100
ccm-manager config
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Multilink1
 bandwidth 1300
 ip address 10.10.1.2 255.255.255.0
 ip tcp header-compression iphc-format
 service-policy output VOICE-POLICY
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
 multilink-group 1
 ip rtp header-compression iphc-format
!
interface FastEthernet0/0
 ip address 10.21.1.1 255.255.255.0
 speed auto
 full-duplex
!
interface Serial0/0
 bandwidth 1300
 no ip address
 encapsulation ppp
 no keepalive
 fair-queue
 ppp multilink
 multilink-group 1
!
 interface FastEthernet0/1
 ip address 10.100.1.2 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
 no ip address
 shutdown
!
interface Serial0/3
```

```
 no ip address
 shutdown
!
router eigrp 1
 network 10.10.1.2 0.0.0.0
 network 10.10.1.0 0.0.0.255
 network 10.21.1.1 0.0.0.0
 auto-summary
 eigrp log-neighbor-changes
!
ip default-gateway 10.10.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
no call rsvp-sync
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
 description afloat FXS 1
 ring cadence pattern08
!
voice-port 1/1/1
!
mgcp
mgcp call-agent 10.21.1.100 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
mgcp package-capability rtp-package
no mgcp package-capability res-package
mgcp package-capability sst-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
dial-peer cor custom
```

```
!
dial-peer voice 999110 pots
 application mgcpapp
 port 1/1/0
!
gateway
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password voip
 login
!
end
```

ASHORE ROUTER CONFIGURATION

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Ashore
!
enable password voip
!
ip subnet-zero
!
no ip domain lookup
!
class-map match-all voice-signaling
  match access-group 103
class-map match-all voice-traffic
  match access-group 102
class-map match-any voip-rtp
   match ip precedence 5
!
policy-map VOICE-POLICY
  class voice-traffic
    priority percent 40
  class voice-signaling
   bandwidth 8
  class class-default
   fair-queue
```

```
!
voice call carrier capacity active
!
voice service voip
 h323
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
voice class h323 1
 h225 timeout tcp establish 3
!
ccm-manager mgcp
ccm-manager music-on-hold
ccm-manager config server 10.11.1.100
ccm-manager config
fax interface-type fax-mail
mta receive maximum-recipients 0
!
interface Multilink1
 bandwidth 1300
 ip address 10.10.1.1 255.255.255.0
 ip tcp header-compression iphc-format
 service-policy output VOICE-POLICY
 no cdp enable
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
 multilink-group 1
 ip rtp header-compression iphc-format
!
interface FastEthernet0/0
 ip address 10.11.1.1 255.255.255.0
 speed auto
 full-duplex
!
interface Serial0/0
 bandwidth 1300
 no ip address
 encapsulation ppp
 fair-queue
 clockrate 1300000
 dce-terminal-timing-enable
 ppp multilink
 multilink-group 1
```

```
!
interface FastEthernet0/1
 ip address 10.100.1.1 255.255.255.0
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
interface Serial0/2
 no ip address
 shutdown
!
interface Serial0/3
 no ip address
 shutdown
!
router eigrp 1
 network 10.10.1.1 0.0.0.0
 network 10.10.1.0 0.0.0.255
 network 10.11.1.1 0.0.0.0
 auto-summary
 eigrp log-neighbor-changes
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
no ip http server
ip pim bidir-enable
!
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
call rsvp-sync
!
voice-port 1/0/0
 description ashore FXS1
 ring cadence pattern04
!
voice-port 1/0/1
!
mgcp
mgcp call-agent 10.11.1.100 2427 service-type mgcp version 0.1
mgcp dtmf-relay voip codec all mode out-of-band
mgcp rtp unreachable timeout 1000 action notify
```

```
mgcp package-capability rtp-package
no mgcp package-capability res-package
mgcp package-capability sst-package
no mgcp timer receive-rtcp
mgcp sdp simple
mgcp fax t38 inhibit
mgcp rtp payload-type g726r16 static
!
mgcp profile default
!
dial-peer cor custom
!
dial-peer voice 999100 pots
 application mgcpapp
 port 1/0/0
!
gateway
!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
 password voip
 login
!
end
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Black, Uyless. Voice Over IP, (Prentice Hall, Upper Saddle River, NJ, 2000)

2. VoIP Fundamentals, A Two-Day Course, TONEX (Tonex, San Jose, CA, 2001)

3. ITU-T Recommendation Q.310, Definition and Function of Signals, (Geneva 1988)

4. Caputo, Robert. Cisco Packetized Voice & Data Integrated, (McGraw-Hill, San Francisco, CA 2000)

5. ITU-T Recommendation H.323, Packet-Based Multimedia Communications Systems, (Geneva 2000)

6. Caputo, Robert. Voice Over IP, (Prentice Hall, Saddle River, NJ, 2000)

7. Elachi, Joanna. Standards Snapshot: The State Of The Big 3 In VoIP Signaling Protocols, (Commweb, November 2000)

8. MGCP Media Gateway Control Protocol, Technical White Paper, (Integral Access, Chelmsford, MA, 2001)

9. Walker, John Q. A Handbook for Successful VoIP Deployment: Network Testing, QoS, and More, (NetIQ Corporation, 2001)

10. Yocom, Betsy, et al. "VoIP Makes Strides," Network World, (January 2002)

11. Yocom, Betsy, et al. "Vendors Pass VoIP Interop Hurdle," Network World, (March 2001: 45-47)

12. "Hoover's Online," http://www.hoovers.com, (April 2002)

13. "Morningstar.com," http://www.morningstar.com, (April 2002)

14. "Yahoo! Finance," http://finance.yahoo.com, (April 2002)

15. "Enterprise Class IP Solutions (ECLIPS)," Avaya IP Call Processing White Paper, (November 2000)

16. "Components of Avaya Enterprise Class IP Solutions," http://www1.avaya.com/enterprise/solutions/convergence/eclips/components.html, (April 2002)

17. "The Enterprise Class IP Solutions Model," http://www1.avaya.com/enterprise/solutions/convergence/eclips/model.html, (April 2002)

18. IP Telephony Technology Evaluation Guide, (Mier Communications Inc., 2001)

19. "MultiService IP Telephony Business Case," http://www.cisco.com/warp/public/cc/so/neso/vvda/iptl/msipt_bc.pdf, (April 2002)

20. Postsecondary Electronic Standards Council, Public Key Infrastructure and Higher Education: An Introduction, (Washington, DC, May 2000)

21. Dorobek, C. and Caternicchia, D., PKI Interoperability 'Paramount', (Federal Computer Week, May 2002)

22. Bart, R., et al., "A Comparison of Voice over IP (VoIP), Asynchronous Transfer Mode (ATM) and Time Domain Multiplexing (TDM) Baseband," (Space and Naval Warfare Systems Command, San Diego, CA, March 2002)

23. Naval Integrated Networks, PMW 158, Presentation, "Automated Digital Network System," (Space and Naval Warfare Systems Command, San Diego, CA, April 2000)

24. ITU Recommendation I.255.3, Multi-Level Precedence and Preemption Service (MLPP), (Geneva 1990)

25. Polk, James M., Internet Engineering Task Force Internet Draft, An Architecture for Multi-Level Precedence and Preemption over IP, http://www.ietf.org/internet-drafts/draft-polk-mlpp-over-ip-01.txt, (November 2001)

26. "Designing the IP Telephony Network," http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/solution/4_design.htm#80278, (May 2002)

27. "Avaya Mission-Critical Solutions – Avaya Call Processing E911 Advantages," http://www.avaya.com/mission_critical/acp911.html, (May 2002)

28. "VoIP over PPP Links with Quality of Service (LLQ / IP RTP Priority, LFI, cRTP)," http://www.cisco.com/warp/public/788/voice-qos/voip-mlppp.html , (August 2002)

29. "Cisco Catalyst 2950-24 and 2950-12 Fast Ethernet Switches," http://www.cisco.com/univercd/cc/td/doc/pcat/ca2950fe.htm - xtocid9 (August 2002)

30. Senge, Peter, The Fifth Discipline, (New York, 1990)

31. Kotter, J. P. and Schlesinger, L. A., "Choosing Strategies for Change," (*Harvard Business Review* (57:2), March-April 1979)

32. Shein, Edgar H., Organizational Psychology, (Prentice-Hall, Englewood Cliffs, NJ, 1972)

33. "Customer Profile – IP Telephony Settles the SCORE," http://www.cisco.com/warp/public/cc/so/neso/vvda/avvid/score_cp.htm, (June 2001)

34. "Cisco IP Telephony Network Guide; Cisco CallManager Clusters" http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/network/ (August 2002)

35. "Cisco IP Keyswitch" http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121yd/121yd_5/ipkeys.htm#xtocid8, (August 2002)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Communication and Information Systems Department
   Space and Naval Warfare Systems Center
   San Diego, California

8. Information Sciences Department
   Naval Postgraduate School
   Monterey, California